

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001年6月7日 (07.06.2001)

PCT

(10) 国際公開番号
WO 01/41356 A1

(51) 国際特許分類: H04L 9/10,
G06F 12/14, G10K 15/02, G06F 13/00

(21) 国際出願番号: PCT/JP00/08544

(22) 国際出願日: 2000年12月1日 (01.12.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/343389 1999年12月2日 (02.12.1999) JP

(71) 出願人(米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP). 株式会社 ピーエフユー (PFU LIMITED) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町字宇野気又98番地の2 株式会社 ピーエフユー内 Ishikawa (JP). 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 古田茂樹 (FURUTA,

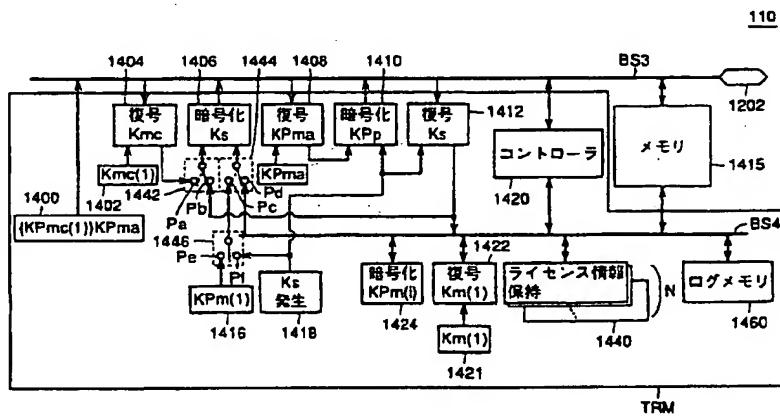
地の2 Ishikawa (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人(米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]. 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 吉川隆敏 (YOSHIKAWA, Takatoshi) [JP/JP]. 武村浩司 (TAKEMURA, Hiroshi) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP). 高橋政幸 (TAKAHASHI, Masataka) [JP/JP]; 〒929-1125 石川県河北郡宇ノ気町字宇野気又98番地の2 株式会社 ピーエフユー内 Ishikawa (JP). 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 古田茂樹 (FURUTA,

/統葉有/

(54) Title: MEMORY CARD AND DATA DISTRIBUTION SYSTEM USING IT

(54) 発明の名称: メモリカードおよびそれを用いたデータ配信システム



1404...DECRYPTION Kmc
1406...ENCRYPTION Ks
1408...DECRYPTION KPma
1410...ENCRYPTION KPp
1412...DECRYPTION Ks
1420...CONTROLLER

1415...MEMORY
1418...Ks GENERATION
1424...ENCRYPTION KPm(i)
1422...DECRYPTION Km(1)
1440...HOLDING OF LICENSE INFORMATION
1460...LOG MEMORY

(57) Abstract: A memory card (110) performs authentication with a server based on data held in an authentication data holding section (1400). The memory card (110) extracts a first session key (Ks1) and a transaction ID from the server by decrypting data placed on a data bus (BS3). Furthermore, the memory card (110) generates a second session key (Ks2) by means of a session key generating section (1418), encrypts the second session key (Ks2) and a key (KPm(1)) unique to the memory card (110) with the first session key (Ks1) and transmits them to the server as keys for encrypting the content key when the content key is decrypted. The transaction ID and the second session key (Ks2) held in a log memory (1460) are used in redistribution.

/統葉有/

WO 01/41356 A1



Shigeki) [JP/JP]. 昌山卓久 (HATAKEYAMA, Takahisa) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP).

(74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, LZ, LC, LK, LR, LS, LT, LU,

LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 國際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイドンスノート」を参照。

(57) 要約:

メモリカード (110) は、認証データ保持部 (1400) に保持されるデータに基づいて、サーバとの間で認証処理を行なう。メモリカード (110) は、データバス (B53) に与えられるデータから、復号処理をすることによりサーバからの第1のセッションキー (Ks1) およびトランザクションIDを抽出する。さらに、メモリカード (110) は、セッションキー発生部 (1418) により第2のセッションキー (Ks2) を生成し、コンテンツキーの復号を受ける際にコンテンツキーを暗号化するための鍵として、第2のセッションキー (Ks2) およびメモリカード (110) に固有な鍵 (Kpm(1)) を第1のセッションキー (Ks1) で暗号化してサーバに送信する。ログメモリ (1460) に保持されるトランザクションIDおよび第2のセッションキー (Ks2) が、再配信処理で使用される。

明細書

メモリカードおよびそれを用いたデータ配信システム

5

技術分野

本発明は、携帯電話等の端末に対して情報を配信するための情報配信システムにおいて、コピーされた情報に対する著作権保護を可能とするメモリカードおよびそれを用いた配信システムに関するものである。

10

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

15

このような情報通信においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

20

つまり、このような情報通信網上において音楽情報や画像データ等の著作者の権利の存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

25

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ところで、上述したようなデジタル情報通信網を介した音楽データなどのコンテンツデータの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

このような記録装置としては、たとえば、メモリカードのように電気的にデータの書き込みおよび消去が可能な媒体が用いられることになる。

さらに、配信された音楽データを再生する装置としては、このようなデータの配信を受けるのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

いずれの場合にしても、デジタル情報通信網、特に無線による通信網を介して音楽データなどのコンテンツデータの配信をうける場合に、音楽データ等の全ての配信が完了する前に、通信回線の状態等によっては、通信が途絶してしまう場合があり得る。たとえば、コンテンツデータを暗号化した暗号化コンテンツデータと復号して再生に必要な再生情報として配信する場合、暗号化コンテンツデータの配信時における通信の途絶に際しては、再接続を行った後、継続してデータの受信を行えばよいが、再生情報の配信に際しては、ユーザに対する課金処理も同時に行われるため、このような通信途絶に対して、ユーザは再接続後に、再生情報の再送信を要求してくることになる。しかしながら、要求に対してむやみに再生情報の再送信を行うことは、著作権者の権利保護の観点から許されるべきでない。逆に、再送信は行わないものとすると、課金処理は行われたにも関わらず、ユーザが再生情報を取得できないというような問題が生じ得る。

20 発明の開示

この発明の他の目的は、再生情報の配信が完了する前に、通信が途絶してしまった場合でも、著作権者の権利を保護した上で通信の再開により、再生情報の配信を完了させることができないデータ配信システムおよびそれに用いられるメモリカードを提供することである。

25 係る目的を達成するために本願発明に係るメモリカードは、暗号化コンテンツデータの再生に関連し、暗号化コンテンツデータを復号して平文にするためのコンテンツキーを含む再生情報を通信経路を介して受けて記録するためのメモリカードであって、データ通信部と、第1の記憶部と、情報抽出部と、第2の記憶部と、制御部とを備える。

データ通信部は、暗号化されて送られる再生情報の受信のために、再生情報の送信元との間での通信経路を確立する。第1の記憶部は、データ通信部から与えられる再生情報に関するデータを保持する。情報抽出部は、データ通信部からの再生情報に関するデータを第1の記憶部へ格納する処理を行い、かつ第1の記憶部に格納されたデータに基づいて、再生情報を抽出する。第2の記憶部は、再生情報の送信処理における処理状態を示す受信ログを記録する。制御部は、メモリカードの動作を制御する。制御部は、要求に応じて受信ログの送信元への送信を制御する。

好ましくは、データ通信部は、第1の鍵保持部と、第1の復号処理部と、第2の鍵保持部と、鍵生成部と、第1の暗号化処理部と、第2の復号処理部とを含む。第1の鍵保持部は、メモリカードに対応して予め定められた第1の公開暗号鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。第1の復号処理部は、再生情報の通信ごとに更新されて送信され、第1の公開暗号鍵によって暗号化された第1の共通鍵を受けて、復号処理する。第2の鍵保持部は、メモリカードごとに異なる第2の公開暗号鍵を保持する。鍵生成部は、再生情報の通信ごとに更新して第2の共通鍵を生成する。第1の暗号化処理部は、第2の公開暗号鍵および第2の共通鍵を、第1の共通鍵に基づいて暗号化し、出力する。第2の復号処理部は、第2の公開暗号鍵で暗号化され、さらに第2の共通鍵で暗号化された再生情報を受け、第2の共通鍵に基づいて復号化する。第1の記憶部は、第2の復号処理部の出力に基づいたデータを保持する。情報抽出部は、第3の鍵保持部と、第3の復号処理部とを含む。第3の鍵保持部は、第2の公開暗号鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する。第3の復号処理部は、再生情報に関するデータの第1の記憶部への格納処理から再生情報を抽出する処理までの過程において、第2の秘密復号鍵についての復号処理を行なう。

この発明のさらに他の局面に従うと、データ配信システムであって、コンテンツデータ供給装置と、複数の端末とを備える。

コンテンツデータ供給装置は、暗号化コンテンツデータと、暗号化コンテンツデータの再生に関する、かつ暗号化コンテンツデータを復号して平文にするため

の復号鍵であるコンテンツキーを含む再生情報とを供給する。コンテンツデータ供給装置は、配信情報保持部と、第1のインターフェース部と、第1のセッションキー発生部と、セッションキー暗号化部と、セッションキー復号部と、第1のライセンスデータ暗号処理部と、第2のライセンスデータ暗号処理部と、配信ログ情報保持部とを含む。配信情報保持部は、コンテンツデータおよび再生情報を保持する。第1のインターフェース部は、外部との間でデータを授受する。第1のセッションキー発生部は、端末に対する再生情報の配信ごとに更新される第1の共通鍵を生成する。セッションキー暗号化部は、ユーザの端末に対応して予め定められた第1の公開暗号鍵により第1の共通鍵を暗号化して第1のインターフェース部に与える。セッションキー復号部は、第1の共通鍵により暗号化されて返信される第2の公開暗号鍵と第2の共通鍵とを復号する。第1のライセンスデータ暗号処理部は、暗号化コンテンツデータを再生するための再生情報を、セッションキー復号部により復号された第2の公開暗号鍵によって暗号化する。第2のライセンスデータ暗号処理部は、第1のライセンスデータ暗号処理部の出力を第2の共通鍵でさらに暗号化して第1のインターフェース部に与え配信する。配信ログ情報保持部は、配信処理中の処理状態を示す配信ログを記録する。複数の端末は、コンテンツデータ供給装置から、通信経路を介して配信を受け、複数のユーザにそれぞれ対応する。各端末は、第2のインターフェース部と、受信制御部と、データ格納部とを含む。第2のインターフェース部は、外部との間でデータ授受をする。受信制御部は、外部との間のデータ授受を制御する。データ格納部は、暗号化コンテンツデータと再生情報を受けて格納する。データ格納部は、第1の鍵保持部と、第1の復号処理部と、第2の鍵保持部と、鍵生成部と、第1の暗号化処理部と、第2の復号処理部と、第1の記憶部と、第3の鍵保持部と、第3の復号処理部と、第2の記憶部とを有する。第1の鍵保持部は、データ格納部に対応して予め定められた第1の公開暗号鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する。第1の復号処理部は、再生情報の通信ごとに更新されて配信され、第1の公開暗号鍵によって暗号化された第1の共通鍵を受けて、復号処理する。第2の鍵保持部は、データ格納部ごとに異なる第2の公開暗号鍵を保持する。鍵生成部は、再生情報の通信ごとに更新して第2の共通鍵を生

成する。第1の暗号化処理部は、第2の公開暗号鍵および第2の共通鍵を、第1の共通鍵に基づいて暗号化し、出力する。第2の復号処理部は、第2の公開暗号鍵で暗号化され、さらに第2の共通鍵で暗号化された再生情報を受け、第2の共通鍵に基づいて復号化する。第1の記憶部は、第2の復号処理部の出力に基づいたデータを保持する。第3の鍵保持部は、第2の公開暗号鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する。第3の復号処理部は、再生情報に関するデータの第1の記憶部への格納処理から再生情報を抽出する処理までの過程において、第2の秘密復号鍵についての復号処理を行なう。第2の記憶部は、暗号化コンテンツデータおよび再生情報の配信処理における処理状態を示す受信ログを記録する。受信制御部は、配信処理中に通信経路が切断された場合に、受信ログに基づいて再配信処理を制御する。

したがって、本発明に係るデータ再生装置を用いた配信システムおよびそれに用いるメモリカードでは、サーバおよびメモリカードがいずれも配信の履歴や配信の状態を保持しているので、通信が配信途中で途絶した場合でも、通信の再開により情報の再送信を可能とし、配信処理の信頼性を向上させることが可能となる。

図面の簡単な説明

図1は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

図3は、ライセンスサーバ10の構成を示す概略ブロック図である。

図4は、携帯電話機100の構成を示す概略ブロック図である。

図5は、メモリカード110の構成を示す概略ブロック図である。

図6は、実施例1に従うデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

図7は、実施例1に従うデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

図8は、実施例1に従うデータ配信システムにおける配信動作を説明するための第3のフローチャートである。

図9は、再接続処理を説明するためのフローチャートである。

図10は、実施例1に従うデータ配信システムにおける、第2の再接続動作を説明するための第1のフローチャートである。

図11は、実施例1に従うデータ配信システムにおける、第2の再接続動作を説明するための第2のフローチャートである。

図12は、実施例1に従うデータ配信システムにおける、第2の再接続動作を説明するための第3のフローチャートである。

図13は、実施例1に従うデータ配信システムにおける第3の再接続動作を説明するためのフローチャートである。

図14は、再接続処理を説明するためのフローチャートである。

図15は、実施例2に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第1のフローチャートである。

図16は、実施例2に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第2のフローチャートである。

図17は、実施例2に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第3のフローチャートである。

図18は、実施例2に従うデータ配信システムにおける、第2の再接続動作を説明するための第1のフローチャートである。

図19は、実施例2に従うデータ配信システムにおける、第2の再接続動作を説明するための第2のフローチャートである。

図20は、実施例2に従うデータ配信システムにおける、第2の再接続動作を説明するための第3のフローチャートである。

図21は、実施例3に従うデータ配信システムにおける、第2の再接続動作を説明するための第1のフローチャートである。

図22は、実施例3に従うデータ配信システムにおける、第2の再接続動作を説明するための第2のフローチャートである。

図23は、実施例3に従うデータ配信システムにおける、第2の再接続動作を

説明するための第3のフローチャートである。

図24は、実施例3に従うデータ配信システムにおける、第2の再接続動作を説明するための第4のフローチャートである。

5 発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

[実施例1]

図1は、本発明のデータ配信システムの全体構成を概略的に説明するための概念図である。

10 なお、以下では携帯電話網を介して音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他のコンテンツデータ、朗読データ、画像データ、映像データ、教材データ等を、他の情報通信網を介して配信する場合にも適用することが可能なものである。

15 図1を参照して、著作権の存在する音楽データを管理するライセンスサーバ10は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、情報を配信するための配信キャリア20である携帯電話会社に、このような暗号化データを与える。一方、認証サーバ12は、コンテンツデータの配信を求めてアクセスしてきたユーザが正規の機器を用いてアクセスしたか否20かの認証を行なう。

携帯電話会社20は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）をライセンスサーバ10に中継する。ライセンスサーバ10は、配信リクエストがあると、認証サーバ12によりユーザが正規の機器からアクセスしていることを確認し、要求された音楽データをさらに暗号化した上で携25帯電話会社20の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

図1においては、たとえば携帯電話ユーザ1の携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取って、上記送

信にあたって行なわれた暗号化については復号した上で、携帯電話機 100 中の音楽再生回路（図示せず）に与える。

さらに、たとえばユーザ 1 は、携帯電話機 100 に接続したヘッドホン 130 等を介してこのような音楽データを「再生」して、聴取することが可能である。

5 以下では、このようなライセンスサーバ 10 と認証サーバ 12 と配信キャリア（携帯電話会社） 20 と併せて、配信サーバ 30 と総称することにする。

また、このような配信サーバ 30 から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

10 このような構成とすることで、まず、メモリカード 110 を所持していないユーザは、配信サーバ 30 からの配信データを受取って再生することができない構成となる。

15 しかも、配信キャリア 20 において、たとえば 1 曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア 20 が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このようなコンテンツデータの配信は、携帯電話網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

20 このとき、たとえばメモリカード 112 を有するユーザ 2 が自己の携帯電話機 102 により、配信サーバ 30 から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量のデータ量を有するコンテンツデータ等をユーザ 2 が直接配信サーバ 30 から受信することとすると、この受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ 1 から、そのコンテンツデータをコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

図 1 に示すように、ユーザ 1 が受信したコンテンツデータを、コンテンツデータ

タそのものおよび当該コンテンツデータを再生可能とするために必要な再生情報とともに、ユーザ2に対してコピーさせる場合を音楽データの「移動」と呼ぶ。この場合に、携帯電話機100および102を介して、メモリカード110と112との間で暗号化されたコンテンツデータおよび再生のために必要な再生情報が移動される。ここで、「再生情報」は、後に説明するように、所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なライセンスキーと、アクセス再生に関する制限情報やコンテンツID等のライセンス情報を有する。

これに対して、再生情報の移動を伴わない、すなわち、コンテンツデータのみをコピーすることを「複製」と呼ぶ。複製では再生情報の移動を伴わないため、複製を受けたユーザは、配信サーバ30に対して再生情報のみの配信を要求すれば、再生できる状態となる。この場合、コンテンツデータの配信における相当量のデータの配信を省くことができる。

このような構成とすることによって、一旦配信サーバより配信を受けたコンテンツデータについて受信者側での柔軟な利用が可能となる。

また、携帯電話機100および102がPHS (Personal Handy Phone) である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ1とユーザ2との間における情報の移動を行なうことが可能である。

図1に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信データを暗号化する方式そのものであり、さらに、第3には、このように配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

本発明の実施例においては、特に、配信中の状態、履歴を情報の送信側および受信側の双方で記録保持し、通信が配信途中で途絶した場合でも、通信の再開により情報の再送信を可能とし、配信処理の信頼性を向上させることができ配信システムについて説明する。

[システムの鍵およびデータの構成]

図2は、図1に示したデータ配信システムにおいて、使用される通信のための

データ、情報等の特性を説明する図である。

まず、配信サーバ30より配信されるデータ Data は、音楽データ等のコンテンツデータである。コンテンツデータ Data は、後に説明するように、少なくともライセンスキーKc によって復号可能な暗号化が施された暗号化コンテンツデータ {Data} Kc という形式で、配信サーバ30よりユーザに配布される。

なお、以下においては、{Y} X という表記は、データ Y を、鍵データ X により復号可能な暗号に変換した情報であることを示すものとする。

さらに、配信サーバからは、コンテンツデータとともに、コンテンツデータに関する、あるいはサーバアクセス関連等の平文情報としての付加情報 Data-inf が配布される。すなわち、付加情報 Data-inf には、コンテンツデータの曲目やアーティスト名などコンテンツデータを特定するための情報や、配信サーバ30が、いずれのサーバであるかを特定するための情報等が含まれる。

次に、コンテンツデータの暗号化や復号・再生処理や、再生回路である携帯電話機や記録媒体であるメモリカードの認証に関わる鍵として、以下のものがある。

すなわち、上述したとおり、暗号化コンテンツデータを復号するためのライセンスキーKc と、コンテンツ再生回路（携帯電話機100）に固有な公開暗号鍵 KPp (n) と、メモリカードに固有な公開暗号鍵 KPmc (m) とがそれぞれ設けられる。

公開暗号鍵 KPp (n) および KPmc (m) により暗号化されたデータは、コンテンツ再生回路（携帯電話機100）の固有の秘密復号鍵 Kp (n) およびメモリカード固有の秘密復号鍵 Kmc (m) によってそれぞれ復号可能である。これら固有の秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる内容を有する。ここで、携帯電話機やメモリカードの種類とは、それらを製造するメーカーや製品の種類や、製造時期（製造ロット）の違い等に基づき規定される。

この公開暗号鍵および秘密復号鍵の付与される単位をクラスと呼ぶものとする。自然数 m、n は、それぞれ各メモリカードおよびコンテンツ再生回路（携帯電話機）のクラスを区別するための番号を表わす。

さらに、配信システム全体で共通に運用される鍵として、主としてライセンスキーKc や後に説明する再生回路に対する制限情報などの取得に利用される秘密

共通鍵 K_{com} と、認証鍵 K_{Pma} とが存在する。秘密共通鍵 K_{com} は、配信サーバと携帯電話機との双方で保持される。

なお、上述したメモリカードおよびコンテンツ再生回路ごとに設定される公開暗号鍵 K_{Pmc} (m) および K_{Pp} (n) は、認証鍵 K_{Pma} にて復号することで、その正当性が確認できる。すなわち認証処理の対象となる認証データ $\{K_{Pmc}$ (m) $\}$ K_{Pma} および $\{K_{Pp}$ (n) $\}$ K_{Pma} の形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。

なお、秘密共通鍵 K_{com} は共通鍵方式に限定されず、公開鍵方式における秘密復号鍵と公開暗号鍵 K_{Pcom} に置き換えて運用することも可能である。この場合、携帯電話機 100 には秘密復号鍵 K_{com} が、配信サーバ 30 には、公開暗号鍵 K_{Pcom} が暗号鍵として保持される。

さらに、システムを構成する機器、すなわち、コンテンツ再生回路である携帯電話機 100 やメモリカード 110 の動作を制御するための情報として、利用者がライセンスキー等を購入する際に、携帯電話機 100 から配信サーバ 30 に対してその購入条件を指定するために送信される購入条件 AC と、購入条件 AC に応じて、配信サーバ 30 からメモリカード 110 に対して配信され、再生のためにライセンスキー K_c にアクセスする回数（再生許諾回数）やライセンスキー K_c の複製・移動回数やコピー、移動に対する制限を示すアクセス制限情報 $AC1$ と、配信サーバ 30 から携帯電話機 100 に対して配信され、再生回路の再生条件の制限を示す再生回路制限情報 $AC2$ とが存在する。再生回路の再生条件とは、たとえば、新曲のプロモーションとして廉価にまたは無償でサンプルを配信する場合などに、各コンテンツデータの冒頭の所定時間のみの再生の許可や再生期限等の条件を意味する。

また、メモリカード 100 内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに個別に設定されるメモリカードごとに固有の公開暗号鍵 K_{Pm} (i) (i・自然数) と、公開暗号鍵 K_{Pm} (i) で暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵 K_m (i) とが存在する。ここで、自然数 i は、各メモリカードを区別するための番号を表わす。

さらに、図 1 に示したデータ配信システムにおいて、データの通信時に使用さ

れる鍵等として以下のものがある。

すなわち、メモリカード外とメモリカード間でのデータ授受における秘密保持のための鍵として、コンテンツデータの配信、再生および移動が行なわれるごとにサーバ30、携帯電話機100または102、メモリカード110または112において生成される共通鍵Ks1～Ks4が用いられる。

ここで、共通鍵Ks1～Ks4は、サーバ、携帯電話もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1～Ks4を「セッションキー」とも呼ぶこととする。

これらのセッションキーKs1～Ks4は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。

具体的には、セッションキーKs1は、配信サーバ30によって配信セッションごとに発生される。セッションキーKs2は、メモリカードによって配信セッションおよび移動（受信側）セッションごとに発生し、セッションキーKs3は、同様にメモリカードにおいて再生セッションおよび移動（送信側）セッションごとに発生する。セッションキーKs4は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

さらに、配信サーバとの間で授受されるデータとしては、コンテンツデータをシステムが識別するためのコンテンツIDや、再生情報の発行がいつ、誰に対して行なわれたかを特定し、配信セッションごとに生成され、各配信セッションを特定するためのコードであるトランザクションIDなどがある。尚、ライセンスIDとトランザクションIDは兼用してもかまわない。

ライセンスID、コンテンツIDおよびアクセス制限情報AC1を総じてライセンス情報と称し、このライセンス情報とライセンスキーKcおよび再生回路制限情報AC2を総じて再生情報と称する。

[ライセンスサーバ10の構成]

図3は、図1に示したライセンスサーバ10の構成を示す概略ブロック図である。

ライセンスサーバ10は、コンテンツデータを所定の方式に従って暗号化した
5 データや、コンテンツID等の配信情報を保持するための情報データベース304と、各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保
持するための課金データベース302と、ライセンスサーバのログ情報を保持す
るためのログ管理データベース306と、情報データベース304、課金データ
ベース302およびログ管理データベース306からのデータをデータバスBS
10 1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を
介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうた
めの通信装置350とを備える。

ここで、ログ管理データベース306に保持されるライセンス情報の配信の履
歴を示す「ライセンス配信ログ」としては、トランザクションID、コンテンツ
15 ID、公開暗号鍵KP_{mc}(n)、KP_p(n)、アクセス制限情報AC1、再生回路制限情報
AC2、公開暗号鍵KP_m(i)、セッションキーKs2、課金状態フラグ等の情報がある。
課金状態フラグは、配信中のコンテンツデータについての課金処理がすでに終了
しているか否かをしめすフラグである。

データ処理部310は、データバスBS1上のデータに応じて、データ処理部
20 310の動作を制御するための配信制御部315と、配信制御部315に制御さ
れて、配信セッション時にセッションキーKs1を発生するためのセッションキー
発生部316と、メモリカードおよび携帯電話機から送られてきた認証のための
認証データ{KP_{mc}(n)}KP_{ma}および{KP_p(n)}KP_{ma}を通信装置350および
データバスBS1を介して受けて、認証鍵KP_{ma}に対する復号処理を行なう復号処
理部312と、セッションキー発生部316より生成されたセッションキーKs1
25 を復号処理部312によって得られた公開暗号鍵KP_{mc}(m)を用いて暗号化して、
データバスBS1に出力するための暗号化処理部318と、各ユーザにおいてセ
ッションキーKs1によって暗号化された上で送信されたデータをデータバスBS
1をより受けて、復号処理を行なう復号処理部320とを含む。

データ処理部 310 は、さらに、秘密共通鍵 K_{com} を保持する K_{com} 保持部 322 と、配信制御部 315 から与えられるライセンスキー K_c および再生回路制限情報 AC_2 を秘密共通鍵 K_{com} によって暗号化する暗号化処理部 324 と、暗号化処理部 324 から出力されたデータを復号処理部 320 によって得られたメモリカード固有の公開暗号鍵 $K_{Pm}(i)$ によって暗号化するための暗号化処理部 326 と、暗号化処理部 326 の出力を、復号処理部 320 から与えられるセッションキー $K_s 2$ によってさらに暗号化してデータバス BS_1 に出力するための暗号化処理部 328 を含む。

なお、秘密共通鍵 K_{com} を非対称な公開鍵暗号系の鍵とする場合においては、
10 鍵データを保持する保持部 322 は、共通鍵方式における秘密共通鍵 K_{com} に代えて公開鍵方式における暗号鍵である公開暗号鍵 K_{Pcom} を保持する。

[携帯電話機 100 の構成]

図 4 は、図 1 に示した携帯電話機 100 の構成を説明するための概略ブロック図である。

15 携帯電話機 100 においては、クラスを表わす自然数 n は、 $n = 1$ とする。

携帯電話機 100 は、携帯電話網により無線伝送される信号を受信するためのアンテナ 1102 と、アンテナ 1102 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、携帯電話機 100 の各部のデータ授受を行なうためのデータバス BS_2 と、データバス BS_2 を介して携帯電話機 100 の動作を制御するためのコントローラ 1106 を含む。

携帯電話機 100 は、さらに、外部からの指示を携帯電話機 100 に与えるためのキーボード 1108 と、コントローラ 1106 等から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データバス BS_2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1112 と、外部との間でデータの授受を行なうためのコネクタ 1120 と、コネクタ 1120 からのデータをデータバス BS_2 に与え得る信号に変換し、または、データバス BS_2 からのデータをコネクタ 1120 に与え得る信号に変換するための外部インターフェース部 1122 を含む。

携帯電話機 100 は、さらに、配信サーバ 30 からのコンテンツデータ（音楽データ）を記憶し、かつ復号処理するための着脱可能なメモリカード 110 と、メモリカード 110 とデータバス BS2 との間のデータの授受を制御するためのメモリインターフェース 1200 と、携帯電話機のクラスごとに設定される公開暗号鍵 KPp (1) を、認証鍵 KPma で復号することで認証可能な状態に暗号化したデータを保持する認証データ保持部 1500 を含む。
5

携帯電話機 100 は、さらに、携帯電話機（コンテンツ再生回路）のクラス固有の復号鍵である秘密復号鍵 Kp (n) (n = 1) を保持する Kp 保持部 1502 と、データバス BS2 から受けたデータを秘密復号鍵 KP (1) によって復号し、メモリカードによって発生されたセッションキー Ks 3 を得る復号処理部 1504 と、メモリカード 110 に記憶されたコンテンツデータの再生を行なう再生セッションにおいて、メモリカード 110 との間でデータバス BS2 上においてやり取りされるデータを暗号化するためのセッションキー Ks 4 を乱数等により発生するセッションキー発生部 1508 と、生成されたセッションキー Ks 4 を復号処理部 1504 によって得られたセッションキー Ks 3 によって暗号化しデータバス BS2 に出力する暗号化処理部 1506 と、データバス BS2 上のデータをセッションキー Ks 4 によって復号して、データ {Kc//AC.2} Kcom を出力する復号処理部 1510 とをさらに含む。
10
15

携帯電話機 100 は、さらに、秘密共通鍵 Kcom を保持する Kcom 保持部 1512 と、復号処理部 1510 が output するデータ {Kc//AC.2} Kcom を秘密共通鍵 Kcom で復号し、ライセンスキー Kc および再生回路制限情報 AC.2 を出力する復号処理部 1514 と、データバス BS2 より暗号化された暗号化コンテンツデータ {Data} Kc を受けて、復号処理部 1514 より取得してライセンスキー Kc によって復号しコンテンツデータ Data を出力する復号処理部 1516 と、復号処理部 1516 の出力であるコンテンツデータ Data を受けて音楽を再生するための音楽再生部 1518 と、音楽再生部 1518 と音声再生部 1112 の出力を受けて、動作モードに応じて選択的に出力するための切換部 1525 と、切換部 1525 の出力を受けて、ヘッドホン 130 と接続するための接続端子 1530 とを含む。
20
25

ここで、復号処理部 1514 から出力される再生回路制限情報 AC2 は、データバス BS2 を介して、コントローラ 1106 に与えられる。

なお、図 4においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては一部割愛している。

5 [メモリカード 110 の構成]

図 5 は、図 1 に示したメモリカード 110 の構成を説明するための概略プロック図である。

既に説明したように、公開暗号鍵 KPm (i) およびこれに対応する秘密復号鍵 Km (i) は、メモリカードごとに固有の値であるが、メモリカード 110 においては、この自然数 $i=1$ であるものとする。また、メモリカードのクラスに固有の公開暗号鍵および秘密復号鍵として、KPmc (m) および Kmc (m) が設けられるが、メモリカード 110 においては、自然数 m は、 $m=1$ で表わされるものとする。

15 メモリカード 110 は、認証データ {KPmc (1)} · KPma を保持する認証データ保持部 1400 と、メモリカードのクラスごとに設定される固有の復号鍵である Kmc (1) を保持する Kmc 保持部 1402 と、メモリカードごとに固有に設定される公開暗号化鍵 KPm (1) を保持する KPm (1) 保持部 1416 と、公開暗号化鍵 KPm (1) によって復号できる非対称な秘密復号鍵 Km (1) を保持する Km (1) 保持部 1421 とを含む。ここで、認証データ保持部 1400 は、メモリカードのクラスごとに設定される公開暗号鍵 KPmc (1) を認証鍵 KPma で復号することでその正当性を認証できる暗号化を行って保持する。

20 メモリカード 110 は、さらに、メモリインタフェース 1200 との間で信号を端子 1202 を介して授受するデータバス BS3 と、データバス BS3 にメモリインタフェース 1200 から与えられるデータから、メモリカードのクラスごとに固有の秘密復号鍵 Kmc (1) を Kmc (1) 保持部 1402 から受けて配信サーバが配信セッションにおいて生成したセッションキー Ks3 を接点 Pa に出力する復号処理部 1404 と、KPma 保持部 1443 から認証鍵 KPma を受けて、データバス BS3 に与えられるデータから認証鍵 KPma による復号処理を実行して復号結

果を暗号化処理部 1410 に出力する復号処理部 1408 と、切換スイッチ 1442 によって選択的に与えられる鍵データによって、切換スイッチ 1444 によって選択的に与えられるデータを暗号化してデータバス BS3 に出力する暗号化処理部 1406 とを含む。

5 メモリカード 110 は、さらに、配信、再生および移動の各セッションにおいてセッションキーを発生するセッションキー発生部 1418 と、セッションキー発生部 1418 の出力したセッションキーを復号処理部 1408 によって得られる公開暗号鍵 KPp (n) によって暗号化してデータバス BS3 に出力する暗号化処理部 1410 と、BS3 より暗号化されたデータを受けてセッションキー発生部 1418 より得たセッションキー Ks3 によって復号し、復号結果をデータバス BS4 に送出する復号処理部 1412 とを含む。

10 メモリカード 110 は、さらに、配信や移動セッション等においてデータバス BS4 上のデータをメモリカード固有の公開暗号鍵 KPm (i) (i は、1 あるいは他のメモリカードの番号 j も可能) で暗号化する暗号化処理部 1424 と、データバス BS4 上のデータを公開暗号鍵 KPm (1) と対をなすメモリカード 110 固有の秘密復号鍵 Km (1) によって復号するための復号処理部 1422 と、公開暗号鍵 KPm (1) で暗号化されている再生情報 (ライセンスキー Kc、コンテンツ ID、トランザクション ID、アクセス制限情報 AC1、再生回路制限情報 AC2) の一部をデータバス BS4 より受けて格納するとともに、暗号化コンテンツデータ (Data) Kc をデータバス BS3 より受けて格納するためのメモリ 1415 とを含む。

15 携帯電話機 110 は、さらに、復号処理部 1422 によって得られるライセンス情報 (トランザクション ID、コンテンツ ID およびアクセス制限情報 AC1) を保持するためのライセンス情報保持部 1440 と、メモリカードにおける再生情報の送受信に関するログを保持するためのログメモリ 1460 と、データバス BS3 を介して外部との間でデータ授受を行ない、データバス BS4 との間で再生情報等を受けて、メモリカード 110 の動作を制御するためのコントローラ 1420 とを含む。

20 ログメモリ 1460 に保持される再生情報の受信状態を示す「受信ログ」とし

では、トランザクションIDやセッションキーKs2等がある。実施例1では、これらの受信ログ情報は、ライセンスの受信が行なわれる際に生成されるデータであり、再生情報のメモリカード110への受信および保存が完了した時点で、消去される。

5 なお、図5において、実線で囲んだ領域TRMは、メモリカード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読み出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスマジュール(Tamper Resistance Module)である。

10 もちろん、メモリ1415も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図5に示したような構成とすることで、メモリ1415中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ1415中のデータのみでは、コンテンツデータから音楽を15 再生することは不可能であり、かつ高価なタンパーレジスタンスマジュール内にメモリ1415を設ける必要がないので、製造コストが低減されるという利点がある。

[配信動作]

20 次に、本発明の実施例に従うデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

図6、図7および図8は、実施例1に従うデータ配信システムにおけるコンテンツデータの購入時に発生する配信動作(以下、配信セッションともいう)を説明するための第1、第2および第3のフローチャートである。

25 図6～図8においては、ユーザ1が、メモリカード110を用いることで、携帯電話機100を介して配信サーバ30から音楽データの配信を受ける場合の動作を説明している。

まず、ユーザ1が、携帯電話機100のキーボード1108のキーの操作等によって、配信リクエストがなされる(ステップS100)。

メモリカード110においては、この配信リクエストに応じて、認証データ保

持部 1400 より認証データ {KPmc (1) } KPma が出力される (ステップ S 1 0 2)。

携帯電話機 100 は、メモリカード 110 から受理した認証のための認証データ {KPmc (1) } KPma に加えて、携帯電話機 100 自身の認証のための認証データ {KPp (1) } KPma と、コンテンツ ID、ライセンス購入条件 AC とを配信サーバ 30 に対して送信する (ステップ S 1 0 4)。

配信サーバ 30 では、携帯電話機 100 からコンテンツ ID、認証データ {KPmc (1) } KPma、{KPp (1) } KPma、ライセンス購入条件 AC を受信し (ステップ S 1 0 6)、復号処理部 312 において認証鍵 KPma で復号処理を実行して、メモリカード 110 の公開暗号鍵である KPmc (1) と、携帯電話機 100 の公開暗号鍵である KPp (1) とを受理する (ステップ S 1 0 8)。

配信制御部 315 は、受理した公開暗号鍵 KPmc (1) および KPp (1) に基づいて、認証サーバ 12 に対して照会を行ない (ステップ S 1 1 0)、これらの公開暗号鍵が有効である場合には次の処理 (ステップ S 1 1 2) に移行し、これらの公開暗号鍵が無効である場合には、処理を終了する (ステップ S 1 7 0)。

ここで、認証鍵 KPma による復号処理において、公開暗号鍵 KPp (1) あるいは KPmc (1) の正当性の認証が行なわれるにあたり、認証サーバ 12 に照会を行うとしたが、公開暗号鍵 KPp (1) あるいは KPmc (1) は、それが認証鍵 KPma によって復号することでその正当性が判断可能な暗号化が施されているため、ライセンスサーバ 10 の配信制御部 315 が認証鍵 KPma による復号結果から独自に認証を行う構成としてもよい。

照会の結果、正規のメモリカードへの配信であることが認識されると、配信制御部 315 は、次に、配信セッションを特定するためのトランザクション ID を生成する (ステップ S 1 1 2)。

照会の結果、正規のメモリカードへの配信であることが確認されると、さらに、配信制御部 315 は、トランザクション ID、コンテンツ ID、公開暗号鍵 KPmc (1)、KPp (1) を、未課金であるとの情報 (課金状態フラグ) とともに、ライセンス配信ログとして管理データベース 306 に記録する (ステップ S 1 1 3)。

続いて、配信サーバ 30 において、セッションキー発生部 316 は、配信のた

めのセッションキー K_{s1} を生成する。セッションキー K_{s1} は、復号処理部 312 によって得られたメモリカード 110 に対応する公開暗号鍵 K_{Pmc} (1) により、暗号化処理部 318 によって暗号化される (ステップ S114)。

5 トランザクション ID と暗号化されたセッションキー $\{K_{s1}\}_{K_{mc}}$ (1) とは、データバス BS1 および通信装置 350 を介して外部に出力される (ステップ S116)。

10 携帯電話機 100 が、トランザクション ID および暗号化されたセッションキー $\{K_{s1}\}_{K_{mc}}$ (1) を受信すると (ステップ S118)、メモリカード 110 においては、メモリインターフェース 1200 を介して、受信データをデータバス BS3 に与える。復号処理部 1404 が、保持部 1402 に保持されるメモリカード 110 固有の秘密復号鍵 K_{mc} (1) により $\{K_{s1}\}_{K_{mc}}$ (1) を復号処理することにより、セッションキー K_{s1} を復号し抽出し、結果、トランザクション ID とセッションキー K_{s1} を受理する (ステップ S120)。

15 ここまで S120 までの処理を、「トランザクション ID 取得ステップ」と呼ぶことにする。

20 図 7 を参照して、コントローラ 1420 は、配信サーバ 30 で生成されたセッションキー K_{s1} の受理を確認すると、セッションキー発生部 1418 に対して、メモリカードにおいて配信動作時に生成されるセッションキー K_{s2} の生成を指示する。さらに、コントローラ 1420 は、セッションキー K_{s2} を、受け取ったトランザクション ID とともに受信

ログとして、ログメモリ 1460 に記録する (ステップ S121)。

25 暗号化処理部 1406 は、切換スイッチ 1442 の接点 P_a を介して復号処理部 1404 より与えられるセッションキー K_{s1} によって、切換スイッチ 1444 および 1446 の接点を順次切換えることによって与えられるセッションキー K_{s2} および公開暗号鍵 K_{Pm} (1) を暗号化して、 $\{K_{s2} // K_{Pm}$ (1) $\}_{K_{s1}}$ をデータバス BS3 に出力する (ステップ S122)。

データバス BS3 に出力された暗号データ $\{K_{s2} // K_{Pm}$ (1) $\}_{K_{s1}}$ は、データバス BS3 から端子 1202 およびメモリインターフェース 1200 を介して携帯電話機 100 に送信され、携帯電話機 100 から配信サーバ 30 に送信される

(ステップ S 1 2 4)。

配信サーバ 3 0 は、暗号化データ $\{Ks2//KPm(1)\} Ks1$ を受信して、復号処理部 3 2 0 においてセッションキー $Ks1$ による復号処理を実行し、メモリカードで生成されたセッションキー $Ks2$ およびメモリカード 1 1 0 固有の公開暗号鍵 $KPm(1)$ を受理する (ステップ S 1 2 6)。

さらに、配信制御部 3 1 5 は、ステップ S 1 0 6 で取得したコンテンツ ID およびライセンス購入条件データ AC に従って、アクセス制限情報 AC1 および再生回路制限情報 AC2 を生成する (ステップ S 1 3 0)。さらに、暗号化コンテンツデータを復号するためのライセンスキー Kc を情報データベース 3 0 4 より取得する (ステップ S 1 3 2)。

配信制御部 3 1 5 は、取得したライセンスキー Kc および再生回路制限情報 AC2 を暗号化処理部 3 2 4 に与える。暗号化処理部 3 2 4 は、 $Kcom$ 保持部 3 2 2 より得られる、秘密共通鍵 $Kcom$ によって、ライセンスキー Kc および再生回路制限情報 AC2 を暗号化する (ステップ S 1 3 4)。

暗号化処理部 3 2 4 が output する暗号化データ $\{Kc//AC2\} Kcom$ と、配信制御部 3 1 5 が output するトランザクション ID、コンテンツ ID およびアクセス制限情報 AC1 とは、暗号化処理部 3 2 6 によって、復号処理部 3 2 0 によって得られたメモリカード 1 1 0 固有の公開暗号鍵 $KPm(1)$ によって暗号化される (ステップ S 1 3 6)。

暗号化処理部 3 2 8 は、暗号化処理部 3 2 6 の出力を受けて、メモリカード 1 1 0 において生成されたセッションキー $Ks2$ によって暗号化する (ステップ S 1 3 7)。

配信制御部 3 1 5 は、ログデータ管理データベース 3 0 6 に、アクセス制限情報 AC1、再生回路制限情報 AC2、公開暗号鍵 $KPm(1)$ 、セッションキー $Ks2$ を、課金済の情報 (課金状態フラグ) とともに記録する (ステップ S 1 3 8)。

暗号化処理部 3 2 8 より出力された暗号化データ $\{(\{Kc//AC2\} Kcom//トランザクション ID//コンテンツ ID//AC1\} Ks2)$ は、データバス BS 1 および通信装置 3 5 0 を介して携帯電話機 1 0 0 に送信される (ステップ S 1 3 9)。

このように、送信サーバおよびメモリカードでそれぞれ生成されるセッション

キーをやりとりし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。さらに、配信サーバ30では、課金状態、配信の履歴に関する情報が記録保持されることになる。

携帯電話機100は、送信された暗号化データ $\{ \{ Kc // AC2 \} Kcom // \text{トランザクションID} // \text{コンテンツID} // AC1 \} Km(1) \} Ks2$ を受信し（ステップS140）、メモリカード110においては、メモリインターフェース1200を介して、データバスBS3に与えられた受信データを復号化処理部1412によって復号する。すなわち、復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてデータバスBS3の受信データを復号しデータバスBS4に出力する（ステップS144）。

図8を参照して、ステップS144の段階で、データバスBS4には、Km(1)保持部1421に保持される秘密復号鍵Km(1)で復号可能なデータ $\{ \{ Kc // AC2 \} Kcom // \text{ライセンスID} // \text{コンテンツID} // AC1 \} Km(1)$ が output されている。このデータ $\{ \{ Kc // AC2 \} Kcom // \text{トランザクションID} // \text{コンテンツID} // AC1 \} Km(1)$ が、まず秘密復号鍵Km(1)により復号され、再生情報であるデータ $\{ Kc // AC2 \} Kcom$ 、トランザクションID、コンテンツID、アクセス制限情報AC1が受理される（ステップS146）。

トランザクションID、コンテンツID、アクセス制限情報AC1が、ライセンス情報保持部1440に記録される。データ $\{ Kc // AC2 \} Kcom$ は、再び、公開暗号鍵KPm(1)により暗号化され、データ $\{ \{ Kc // AC2 \} Kcom \} Km(1)$ としてメモリ1415に格納される（ステップ）。

さらに、ログメモリ1460中の受信ログは消去される（ステップS150）。ステップS121からステップS150までの処理を「再生情報取得ステップ」と呼ぶことにする。この「再生情報取得ステップ」では、課金対象の処理を行なう。

ステップS150までの処理が正常に終了した段階で、携帯電話機100から

配信サーバ30にコンテンツデータの配信要求がなされる（ステップS152）。

配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ{Data}Kcおよび付加情報DATA-infを取得して、これらのデータをデータバスBS1および通信装置350を介して出力する（ステップS154）。

携帯電話機100は、{Data}Kc//Data-infを受信して、暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infを受理する（ステップS156）。暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infはメモリインタフェース1200および端子1,202を介してメモリカード110のデータバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infがそのままメモリ1415に格納される（ステップS158）。

ステップS152からステップS158までの処理を「コンテンツデータ取得ステップ」と呼ぶことにする。この「コンテンツデータ取得ステップ」では、課金対象外の処理を行なう。

さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され（ステップS160）、配信サーバ30で配信受理を受信すると（ステップS162）、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され（ステップS164）、配信サーバの処理が終了する（ステップS170）。

[再接続動作]

つづいて、以上説明した配信動作のいずれか処理ステップの段階で、通信回線が途絶した場合に、再度、配信を受けるために再接続が行なわれる場合の処理を説明する。図9は、再接続処理を説明するためのフローチャートである。

まず、たとえば、ユーザ1が、携帯電話機100のキーボード1108のキーの操作等によって、再接続のリクエストがなされ、再接続処理が開始される（ステップS200）。

つづいて、携帯電話機100のコントローラ1106は、通信が切断したステップが、いずれの処理中であったかを判断し（ステップS202）、それがトラ

ンザクション ID 取得ステップであれば、課金の対象となっていないので図 6～図 8 の基本配信処理（第 1 の再接続処理）を再度やり直し（ステップ S 204）、再接続処理が終了する（ステップ S 206）。

一方、コントローラ 1106 は、通信が切断したステップが、ライセンス取得ステップであれば（ステップ S 202）、後に説明する受信ログに基づく第 2 の再接続処理を行ない（ステップ S 206）、または、コンテンツデータ取得ステップであれば（ステップ S 202）、後に説明する通信の切断時における通信を継続して行うための第 3 の再接続処理を行ない（ステップ S 206）、再接続処理が終了する（ステップ S 210）。

10 [第 2 の再接続処理]

図 10、図 11 および図 12 は、実施例 1 に従うデータ配信システムにおける、上述した第 2 の再接続動作を説明するための第 1、第 2 および第 3 のフローチャートである。ライセンスサーバ 10 のライセンス配信ログとメモリカード 110 の受信ログを対比することで、通信切断時における再生情報の配信状態を確認し、著作権者の権利を保護しつつ、ユーザへの保証を実現するものである。

15 まず、図 10 を参照して、ユーザ 1 が携帯電話機 100 のキーボード 1108 のキーボタンの操作等によって、再接続リクエストがなされ、これに応じて第 2 の再接続処理が開始される（ステップ S 300）。

メモリカード 110 においては、この再接続リクエストに応じて、ログメモリ 20 1460 に保持されたトランザクション ID が output される（ステップ S 302）。

携帯電話機 100 は、メモリカード 110 から受理したトランザクション ID を配信サーバ 30 に対して送信する（ステップ S 304）。

配信サーバ 30 では、トランザクション ID を受信し（ステップ S 306）、配信制御部 315 が、ログ管理データベース 306 中のライセンス配信ログを検 25 索する（ステップ S 308）。

配信制御部 315 は、受信したトランザクション ID から再接続の要求をしてきた端末（携帯電話機 100 およびメモリカード 110）に対して課金処理がすでにに行なわれている場合（ステップ S 308）、ライセンス配信ログから公開暗号鍵 KPmc (1) を取得する（ステップ S 310）。

セッションキー発生部 316 は、配信のためのセッションキー Ks_1 を生成する。セッションキー Ks_1 は、公開暗号鍵 $KP_{mc}(1)$ により、暗号化処理部 318 によって暗号化される（ステップ S312）。

5 トランザクション ID と暗号化されたセッションキー $\{Ks_1\}_{Kmc}(1)$ とは、データバス BS1 および通信装置 350 を介して外部に出力される（ステップ S314）。

10 携帯電話機 100 が、トランザクション ID および暗号化されたセッションキー $\{Ks_1\}_{Kmc}(1)$ を受信すると（ステップ S316）、メモリカード 110 においては、メモリインターフェース 1200 を介して、データバス BS3 に与えられた受信データを、復号処理部 1404 が、保持部 1402 に保持されるメモリカード 110 固有の秘密復号鍵 $Kmc(1)$ により復号処理することにより、セッションキー Ks_1 を復号し抽出する（ステップ S318）。

以後は、図 7 に示したステップ S121 以降の処理、すなわち、ライセンス取得ステップ以降の処理と同様の処理が行なわれる。

15 一方、ステップ 308 において、配信制御部 315 が、ログ管理データベース 306 中のライセンス配信ログを検索した結果、課金処理が終了していないと判断すると、ライセンス配信ログから公開暗号鍵 $KP_{mc}(1)$ を取得する（ステップ S330）。

20 続いて、配信サーバ 30 において、セッションキー発生部 316 は、配信のためのセッションキー Ks_1 を生成する。セッションキー Ks_1 は、公開暗号鍵 $KP_{mc}(1)$ により、暗号化処理部 318 によって暗号化される（ステップ S332）。

トランザクション ID と暗号化されたセッションキー $\{Ks_1\}_{Kmc}(1)$ とは、データバス BS1 および通信装置 350 を介して外部に出力される（ステップ S334）。

25 携帯電話機 100 が、トランザクション ID および暗号化されたセッションキー $\{Ks_1\}_{Kmc}(1)$ を受信すると（ステップ S336）、メモリカード 110 においては、メモリインターフェース 1200 を介して、データバス BS3 に与えられた受信データを、復号処理部 1404 が、保持部 1402 に保持されるメモリカード 110 固有の秘密復号鍵 $Kmc(1)$ により復号処理することにより、セ

ッションキーKs1を復号し抽出する（ステップS338）。

暗号化処理部1406は、受信ログをセッションキーKs1で暗号化し、
（受信ログ）Ks1を生成する（ステップS340）。

図11を参照して、コントローラ1420は、セッションキー発生部1418
5 に対して、メモリカードにおいて配信動作時に生成されるセッションキーKs2
の生成を指示する（ステップS342）。

暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理
部1404より与えられるセッションキーKs1によって、切換スイッチ1444
および1446の接点を介して与えられるセッションキーKs2¹を暗号化して、
10 {Ks2¹}Ks1を生成する。以上のようにして生成されたデータ（受信ログ）
Ks1および{Ks2¹}Ks1がメモリカード110から出力される（ステップS3
44）。

データバスBS3に出力された暗号データ（受信ログ）Ks1および{Ks2¹}Ks
1は、データバスBS3から端子1202およびメモリインタフェース1200
15 を介して携帯電話機100に送信され、携帯電話機100から配信サーバ30に
送信される（ステップS346）。

配信サーバ30は、暗号化データ（受信ログ）Ks1および{Ks2¹}Ks1を受
信して、復号処理部320においてセッションキーKs1による復号処理を実行し、
受信ログおよびメモリカードで生成されたセッションキーKs2¹を受理する（ス
テップS348）。

続いて、配信制御部315は、受理した受信ログの正当性のチェックを行なう
(ステップS350)。

受信ログが正当でないと判断されると、第2の再接続処理は終了する（ス
テップS390）。

一方、受信ログが正当であると判断されると、配信制御部315は、ライセン
ス配信ログからコンテンツID、アクセス制限情報AC1、再生回路制限情報AC2、
および公開暗号鍵KPm(1)を取得する（ステップS352）。さらに、暗号化コ
ンテンツデータを復号するためのライセンスキーKcを情報データベース304
より取得する（ステップS354）。

配信制御部 315 は、取得したライセンスキー K_c および再生回路制限情報 AC_2 を暗号化処理部 324 に与える。暗号化処理部 324 は、 K_{com} 保持部 322 より得られる、秘密共通鍵 K_{com} によって、ライセンスキー K_c および再生回路制限情報 AC_2 を暗号化する（ステップ S 356）。

5 暗号化処理部 324 が output する暗号化データ $\{K_c//AC_2\} K_{com}$ と、配信制御部 315 が output するトランザクション ID、コンテンツ ID およびアクセス制限情報 AC_1 とは、暗号化処理部 326 によって、ステップ S 352 において得られたメモリカード 110 固有の公開暗号鍵 $K_{Pm}(1)$ によって暗号化される（ステップ S 358）。

10 暗号化処理部 328 は、暗号化処理部 326 の出力を受けて、メモリカード 110 において生成されたセッションキー K_{s2}' によって暗号化する（ステップ S 360）。

15 暗号化処理部 328 より出力された暗号化データ $\{(\{K_c//AC_2\} K_{com} // \text{トランザクション ID} // \text{コンテンツ ID} // AC_1) K_{m}(1)\} K_{s2}'$ は、データバス BS 1 および通信装置 350 を介して携帯電話機 100 に送信される（ステップ S 362）。

20 携帯電話機 100 は、送信された暗号化データ $\{(\{K_c//AC_2\} K_{com} // \text{トランザクション ID} // \text{コンテンツ ID} // AC_1) K_{m}(1)\} K_{s2}'$ を受信し（ステップ S 364）する。

25 図 12 を参照して、メモリカード 110 においては、メモリインターフェース 1200 を介して、データバス BS 3 に与えられた受信データを復号化処理部 1412 によって復号する。すなわち、復号処理部 1412 は、セッションキー発生部 1418 から与えられたセッションキー K_{s2}' を用いてデータバス BS 3 の受信データを復号しデータバス BS 4 に出力する（ステップ S 366）。

この段階で、データバス BS 4 には、 $K_m(1)$ 保持部 1421 に保持される秘密復号鍵 $K_m(1)$ で復号可能なデータ $\{K_c//AC_2\} K_{com} // \text{ライセンス ID} // \text{コンテンツ ID} // AC_1 K_m(1)$ が output されている。このデータ $\{K_c//AC_2\} K_{com} // \text{トランザクション ID} // \text{コンテンツ ID} // AC_1 K_m(1)$ が、まず秘密復号鍵 $K_m(1)$ により復号され、再生情報であるデータ $\{K_c//AC_2\} K_{com}$ 、トランザクシ

ション ID、コンテンツ ID、アクセス制限情報 AC1 が受理される（ステップ S 3 6 8）。

トランザクション ID、コンテンツ ID、アクセス制限情報 AC1 が、ライセンス情報保持部 1 4 4 0 に記録される。データ $\{Kc//AC2\} Kcom$ は、再び、秘密復号鍵 $KPm(1)$ により暗号化され、データ $\{ \{Kc//AC2\} Kcom \} Km(1)$ としてメモリ 1 4 1 5 に格納される（ステップ S 3 7 0）。

さらに、ログメモリ 1 4 6 0 中の受信ログが消去される（ステップ S 3 7 2）。

ステップ S 3 7 2 までの処理が正常に終了した段階で、携帯電話機 1 0 0 から配信サーバ 3 0 にコンテンツデータの配信要求がなされる（ステップ S 3 7 4）。

配信サーバ 3 0 は、コンテンツデータの配信要求を受けて、情報データベース 3 0 4 より、暗号化コンテンツデータ $\{Data\} Kc$ および付加情報 DATA-inf を取得して、これらのデータをデータベース BS 1 および通信装置 3 5 0 を介して出力する（ステップ S 3 7 6）。

携帯電話機 1 0 0 は、 $\{Data\} Kc//Data-inf$ を受信して、暗号化コンテンツデータ $\{Data\} Kc$ および付加情報 Data-inf を受理する（ステップ S 3 7 8）。暗号化コンテンツデータ $\{Data\} Kc$ および付加情報 Data-inf はメモリインタフェース 1 2 0 0 および端子 1 2 0 2 を介してメモリカード 1 1 0 のデータベース BS 3 に伝達される。メモリカード 1 1 0 においては、受信した暗号化コンテンツデータ $\{Data\} Kc$ および付加情報 Data-inf がそのままメモリ 1 4 1 5 に格納される（ステップ S 3 8 0）。

さらに、メモリカード 1 1 0 から配信サーバ 3 0 へは、配信受理の通知が送信され（ステップ S 3 8 2）、配信サーバ 3 0 で配信受理を受信すると（ステップ S 3 8 4）、配信終了の処理が実行され（ステップ S 3 8 6）、配信サーバの処理が終了する（ステップ S 3 9 0）。

25 [第 3 の再接続処理]

図 1 3 は、実施例 1 に従うデータ配信システムにおける、上述した第 3 の再接続動作を説明するためのフローチャートである。

図 1 3 を参照して、ユーザ 1 が、携帯電話機 1 0 0 のキーボード 1 1 0 8 のキー ボタンの操作等によって、再接続リクエストがなされ、これに応じて第 3 の再

接続処理が開始される（ステップS400）。

携帯電話機100においては、この再接続リクエストに応じて、配信サーバ30にコンテンツデータの配信要求がなされる（ステップS402）。

5 配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ{Data}Kcおよび付加情報DATA-infを取得して、これらのデータをデータバスBS1および通信装置350を介して出力する（ステップS404）。

携帯電話機100は、{Data}Kc//Data-infを受信して、暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infを受理する（ステップS406）。

10 暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infはメモリインタフェース1200および端子1202を介してメモリカード110のデータバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ{Data}Kcおよび付加情報Data-infがそのままメモリ1415に格納される（ステップS408）。

15 さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され（ステップS410）、配信サーバ30で配信受理を受信すると（ステップS412）、配信終了の処理が実行され（ステップS414）、配信サーバの処理が終了する（ステップS416）。

[再接続動作中に回線が切断した場合の再接続動作]

20 つづいて、以上説明した再接続動作のいずれか処理ステップの段階で、通信回線が途絶した場合に、さらに再度、配信を受けるために再接続が行なわれる場合の処理を説明する。図14は、このような再接続処理を説明するためのフローチャートである。

25 まず、たとえば、ユーザ1が、携帯電話機100のキーボード1108のキーボタンの操作等によって、再接続のリクエストがなされ、再接続処理が開始される（ステップS500）。

つづいて、メモリカード110中に保持されたライセンス受信待ちログに基づいて、コントローラ1106は、通信が切断したステップが、いずれの処理中であったかを判断し（ステップS502）、それがライセンス取得ステップまたは

再ライセンス取得ステップであれば、第2の再接続処理を再度やり直し（ステップS504）、再接続処理が終了する（ステップS508）。

一方、コントローラ1106は、通信が切断したステップが、コンテンツデータ取得ステップであれば（ステップS502）、後に説明する第3の再接続処理を行ない（ステップS506）、再接続処理が終了する（ステップS508）。

5 このような構成とすることにより、いずれの処理ステップにおいて通信回線が途絶した場合でも、再接続を行なうことが可能で、システムの信頼性が一層強化される。

【実施例2】

10 実施例2のデータ配信システムにおいては、実施例1のデータ配信システムの構成と異なって、以下に説明するように、メモリカード110中のログメモリ1460に保持されたライセンス受信待ちログを消去しない点を特徴とする。このような変更を行なう結果、受信ログには、実施例1の構成に加えて、さらに、受信状態フラグが付け加わる構成となっている。

15 したがって、以下に説明するように実施例2のデータ配信システムの構成は、メモリカード110中のコントローラ1420の動作およびログメモリ1460に保持されるデータが実施例1の場合と異なる。

20 図15、図16および図17は、実施例2に従うデータ配信システムにおけるコンテンツの購入時に発生する配信動作を説明するための第1、第2および第3のフローチャートであり、実施例1の図6～8と対比される図である。

図15～図17においても、ユーザ1が、メモリカード110を用いることで、携帯電話機100を介して配信サーバ30から音楽データの配信を受ける場合の動作を説明している。

25 実施例1のフローと異なる点は、トランザクションID取得ステップの後に、図16に示した、ステップS121では、コントローラ1420は、配信サーバ30で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対して、メモリカードにおいて配信動作時に生成されるセッションキーKs2の生成を指示する。さらに、コントローラ1420は、セッションキーKs2、受け取ったトランザクションIDとともに、受信待ちを示すオン状態と

なった受信状態フラグを受信ログとして、ログメモリ 1460 に記録する（ステップ S121'）。

また、図 17 を参照して、ステップ S148 において、トランザクション ID、コンテンツ ID、アクセス制限情報 AC1 が、ライセンス情報保持部 1440 に記録される。データ $\{Kc//AC2\} Kcom$ は、再び、公開暗号鍵 $KPm(1)$ により暗号化され、データ $\{ \{Kc//AC2\} Kcom \} Km(1)$ としてメモリ 1415 に格納された後、ログメモリ 1460 中の受信ログ中の受信状態フラグは受信済みを示すオフ状態とされる（ステップ S150'）。

その他の処理は、実施例 1 と同様であるので、同一処理には同一符号を付して、
その説明は繰り返さない。

[再接続動作]

実施例 2 においても、実施例 1 の図 9 と同様に、以上説明した配信動作のいずれか処理ステップの段階で、通信回線が途絶した場合に、再度、配信を受けるために再接続処理が行なわれる。

ただし、実施例 1 の場合の第 2 の再接続処理の一部に変更が生じる。

[第 2 の再接続処理]

図 18、図 19 および図 20 は、実施例 2 に従うデータ配信システムにおける、上述した第 2 の再接続動作を説明するための第 1、第 2 および第 3 のフローチャートであり、実施例 1 の図 10～図 12 と対比される図である。

実施例 1 の処理と異なる点は、図 18 において、ステップ S318 においてセシションキー $Ks1$ を受理した後は、図 16 に示したステップ S121' に処理が移行する構成となっている点と、図 20 において、ステップ S370 において、トランザクション ID、コンテンツ ID、アクセス制限情報 AC1 が、ライセンス情報保持部 1440 に記録される。データ $\{Kc//AC2\} Kcom$ は、再び、公開暗号鍵 $KPm(1)$ により暗号化され、データ $\{ \{Kc//AC2\} Kcom \} Km(1)$ としてメモリ 1415 に格納した後、ステップ S372' において、受信ログの受信状態フラグを受信済みを示すオフ状態とする処理を行なう構成となっている点である。

その他の処理は、実施例 1 と同様であるので、同一処理には同一符号を付して、その説明は繰り返さない。

さらに、第3の再接続処理や、再接続動作中に回線が切断した場合の再接続動作については、実施例1の処理と同様である。

以上のような構成とすることでも、いずれの処理ステップにおいて通信回線が途絶した場合でも、再接続を行なうことが可能で、システムの信頼性が一層強化

5 される。

[実施例3]

実施例3のデータ配信システムにおいては、実施例2のデータ配信システムの構成と異なって、以下に説明するように、メモリカード110中のログメモリ1460に保持する受信ログに、状態フラグを加えた状態情報をサーバに送信する構成となっている点である。

10 状態情報は、受信ログであるトランザクションID、セッションキーKs2、受信状態フラグと状態フラグという情報を含む。

ここで、ライセンス状態フラグは、3状態をとるフラグ変数であり、メモリカード110中のライセンス情報保持部1440に受信ログに記録されたトランザクションIDが存在し、対応する再生情報が存在し、かつ、ライセンス情報保持部1440に保持されるアクセス制限情報によって再生が禁止されていない、すなわち、再生可能な場合は、「01h」という値をとり、ライセンス情報保持部にトランザクションIDが存在し、対応する再生情報が無いか、ライセンス情報保持部1440に保持されるアクセス制限情報によって再生が禁止されていて再生できない場合には、「00h」という値をとり、トランザクションIDが存在しない場合には、「FFh」という値をとる。

したがって、以下に説明するように実施例3のデータ配信システムの構成は、メモリカード110中のコントローラ1420の動作およびログメモリ1460に保持されるデータが実施例2の場合と異なる。

25 実施例3の配信動作および再接続動作は、以下に説明する第2の再接続処理を除いては、実施例2の処理と同様であるので、その説明は繰り返さない。

[第2の再接続処理]

図21、図22、図23および図24は、実施例3に従うデータ配信システムにおける、第2の再接続動作を説明するための第1、第2、第3および第4のフ

ローチャートである。

まず、図21を参照して、ステップS300からステップS338までは、実施例2の第2の再接続動作と同様である。

ステップS338において、メモリカード110において、メモリインターフェース1200を介して、データバスBS3に与えられた受信データを、復号処理部1404が、保持部1402に保持されるメモリカード110固有の秘密復号鍵Kmc(1)により復号処理することにより、セッションキーKs1を復号し抽出した後、メモリカード110中のコントローラ1420は、ログメモリ1460中に保持された受信ログ中のトランザクションIDに従って、ライセンス情報保持部1440中に格納されているデータの検索を行なう(ステップ640)。

コントローラ1420は、まず、ライセンス情報保持部1440にトランザクションIDが存在するかをチェックする(ステップS642)。

トランザクションIDが存在しない場合、ライセンス状態フラグを「FFh」に設定し(ステップS644)、処理はステップS652へ移行する。

一方、ステップS642において、トランザクションIDが存在する場合、さらに、コントローラ1420は、ライセンス情報保持部1440に保持されたアクセス制限情報AC1の状態やメモリ1415内に対応するライセンスキーKcが記録されているか否かを確認する(ステップS646)。再生が可能な場合はライセンス状態フラグを「01h」に設定する(ステップS648)。一方、再生できない場合は、ライセンス状態フラグを「00h」に設定する(ステップS650)。その上で、処理はステップS652へ移行する。

続いて、ログメモリ1460の保持されている受信ログに状態フラグを付加した状態情報を生成する(ステップS652)。

コントローラ1420は、セッションキー発生部1418に対して、メモリカードにおいて配信動作時に生成されるセッションキーKs2'の生成を指示する(ステップS654)。

暗号化処理回路1406は、状態情報とセッションキーKs2'をセッションキーKs1で暗号化し、暗号化データ(状態情報//Ks2')Ks1を生成する(ステップS656)。

コントローラ 1420 は、暗号化データ {状態情報//Ks2'} Ks1 に対するハッシュ関数にしたがったハッシュ値を求め、暗号化データ {状態情報//Ks2'} Ks1 に対する署名データ hash を生成する (ステップ S 658)。

5 暗号化処理部 1406 は、切換スイッチ 1442 の接点 Pa を介して復号処理部 1404 より与えられるセッションキー Ks1 によって、コントローラ 1420 の制御のもと与えられる署名データ hash を暗号化して暗号化署名データ {hash} Ks1 を生成する (ステップ S 660)。

10 以上のようにして生成されたデータ {状態情報//Ks2'} Ks1 および暗号化署名データ {hash} Ks1 がメモリカード 110 から出力される (ステップ S 662)。

データバス BS3 に出力された暗号データ {状態情報//Ks2'} Ks1 および暗号化署名データ {hash} Ks1 は、データバス BS3 から端子 1202 およびメモリインターフェース 1200 を介して携帯電話機 100 に送信され、携帯電話機 100 から配信サーバ 30 に送信される (ステップ S 664)。

15 配信サーバ 30 は、暗号化データ {状態情報//Ks2'} Ks1 および暗号化署名データ {hash} Ks1 を受信する (ステップ S 666)。

図 23 を参照して、配信サーバ 30 の復号処理部 320 において暗号化署名データ {hash} Ks1 に対してセッションキー Ks1 による復号処理を実行し、暗号データ {状態情報//Ks2'} Ks1 に対する署名データ hash を得る。続いて、暗号データ {状態情報//Ks2'} Ks1 と署名データから、状態情報の正当性をチェックする (ステップ S 668)。

25 状態情報が正当でないならば処理は終了し (ステップ S 712)、状態情報が正当であると確認されると、セッションキー Ks1 による復号処理を実行し、状態情報およびメモリカードで生成されたセッションキー Ks2' を受理する (ステップ S 670)。

統いて、配信制御部 315 は、受理した状態情報とライセンス配信ログに基づいて再生情報の再送要求の正当性のチェックを行なう (ステップ S 672)。

再生情報の再送要求が正当でないと判断されると、第 2 の再接続処理は終了する (ステップ S 712)。

一方、再生情報の再送要求が正当であると判断されると、配信制御部 315 は、ライセンス配信ログからコンテンツ ID、アクセス制限情報 AC1、再生回路制限情報 AC2、および公開暗号鍵 KPm(1) を取得する（ステップ S 674）。さらに、暗号化コンテンツデータを復号するためのライセンスキー Kc を情報データベース 304 より取得する（ステップ S 676）。

配信制御部 315 は、取得したライセンスキー Kc および再生回路制限情報 AC2 を暗号化処理部 324 に与える。暗号化処理部 324 は、Kcom 保持部 322 より得られる、秘密共通鍵 Kcom を用いて、ライセンスキー Kc および再生回路制限情報 AC2 を暗号化する（ステップ S 678）。

10 暗号化処理部 324 が output する暗号化データ $\{Kc//AC2\} Kcom$ と、配信制御部 315 が output する トランザクション ID、コンテンツ ID およびアクセス制限情報 AC1 とは、暗号化処理部 326 によって、ステップ S 674 において得られたメモリカード 110 固有の公開暗号鍵 KPm(1) によって暗号化される（ステップ S 680）。

15 暗号化処理部 328 は、暗号化処理部 326 の出力を受けて、メモリカード 110 において生成されたセッションキー Ks2⁻ によって暗号化する（ステップ S 682）。

暗号化処理部 328 より出力された暗号化データ $\{ \{ \{Kc//AC2\} Kcom // \text{トランザクション ID} // \text{コンテンツ ID} // AC1 \} Km(1) \} Ks2^-$ は、データバス BS1 および通信装置 350 を介して携帯電話機 100 に送信される（ステップ S 684）。

携帯電話機 100 は、送信された暗号化データ $\{ \{ \{Kc//AC2\} Kcom // \text{トランザクション ID} // \text{コンテンツ ID} // AC1 \} Km(1) \} Ks2^-$ を受信し（ステップ S 686）する。

25 図 2.4 を参照して、メモリカード 110 においては、メモリインターフェース 1200 を介して、データバス BS3 に与えられた受信データを復号化処理部 1412 によって復号する。すなわち、復号処理部 1412 は、セッションキー発生部 1418 から与えられたセッションキー Ks2⁻ を用いてデータバス BS3 の受信データを復号しデータバス BS4 に出力する（ステップ S 690）。

この段階で、データバス BS 4 には、Km (1) 保持部 1421 に保持される秘密復号鍵 Km (1) で復号可能なデータ { {Kc//AC2} Kcom//ライセンス ID//コンテンツ ID//AC1} Km(1) が出力されている。このデータ { {Kc//AC2} Kcom//トランザクション ID//コンテンツ ID//AC1} Km(1) が、まず公開暗号鍵 Km(1) により復号され、データ {Kc//AC2} Kcom、トランザクション ID、コンテンツ ID、アクセス制限情報 AC1 が受理される (ステップ S 692)。

トランザクション ID、コンテンツ ID、アクセス制限情報 AC1 が、ライセンス情報保持部 1440 に記録される。データ {Kc//AC2} Kcom は、再び、公開暗号鍵 KPm(1) により暗号化され、データ { {Kc//AC2} Kcom} Km(1) としてメモリ 1415 に格納される (ステップ S 694)。

さらに、ログメモリ 1460 中の受信ログ中の受信状態フラグ受信済みを示すオフ状態に変更される (ステップ S 696)。

ステップ S 372までの処理が正常に終了した段階で、携帯電話機 100 から配信サーバ 30 にコンテンツデータの配信要求がなされる (ステップ S 698)。

配信サーバ 30 は、コンテンツデータの配信要求を受けて、情報データベース 304 より、暗号化コンテンツデータ {Data} Kc および付加情報 DATA-inf を取得して、これらのデータをデータバス BS 1 および通信装置 350 を介して出力する (ステップ S 700)。

携帯電話機 100 は、{Data} Kc//Data-inf を受信して、暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf を受理する (ステップ S 702)。

暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf はメモリインタフェース 1200 および端子 1202 を介してメモリカード 110 のデータバス BS 3 に伝達される。メモリカード 110 においては、受信した暗号化コンテンツデータ {Data} Kc および付加情報 Data-inf がそのままメモリ 1415 に格納される (ステップ S 704)。

さらに、メモリカード 110 から配信サーバ 30 へは、配信受理の通知が送信され (ステップ S 706)、配信サーバ 30 で配信受理を受信すると (ステップ S 708)、配信終了の処理が実行され (ステップ S 710)、配信サーバの処理が終了する (ステップ S 712)。

なお、以上の説明では、ステップS654において、状態情報の全ての情報をセッションキーK_s1で暗号化して、ステップS622およびS624により、配信サーバ30に対して、暗号化データ {状態情報//K_s2'} K_s1が送信される構成となっている。

5 しかしながら、状態情報のうちトランザクションIDについては、その機密というよりは、その出所が明らかであれば良い情報である。したがって、暗号化署名データ {hash} K_s1によって、その出所が明らかとなるので、このトランザクションIDについては暗号化せず、平文のままで配信サーバ30に送信される構成でもよい。この場合、状態情報は、トランザクションID// {トランザクションIDを除く状態情報//K_s2'} K_s1として送信されることとなり、署名データh_as_hはこれに対して生成される。

以上のような構成とすることでも、いずれの処理ステップにおいて通信回線が途絶した場合でも、再接続を行なうことが可能で、システムの信頼性が一層強化される。

10 15 さらに、実施例1～3のデータ配信システムでは、配信サーバ30および携帯電話機100において秘密共通鍵K_{com}による暗号化および復号処理が行なわれる構成となっていたが、この秘密共通鍵K_{com}による暗号化および復号処理を用いない構成とすることも可能である。

すなわち、図3において説明した、実施例1のデータ配信システムが具備する配信サーバ30において、K_{com}保持部322と暗号化処理部324を具備しない構成とすることが可能である。すなわち、このような配信サーバ30においては、配信制御部315が出力するライセンスキーK_cおよび再生回路制限情報AC2は、直接暗号化処理部326に伝達される。

20 25 さらに、実施例1の図4で説明した携帯電話機100の構成と比較して、秘密共通鍵K_{com}を保持するK_{com}保持部1512と秘密共通鍵K_{com}による復号処理部1514を具備しない構成とすることが可能である。

すなわち、このような構成の携帯電話機101においては、配信サーバ30において秘密共通鍵を対称な暗号鍵として暗号化処理が施されていないことに対応して、セッションキーK_s4による復号処理を実行する復号処理部1510によっ

て直接ライセンスキー K_c が得られるため、これを復号処理部 1510 に直接与える構成となる。

また、このように秘密共通鍵 K_{com} による暗号化および復号処理を用いない構成においても、メモリカード 110 はそのまま用いることができる。

5 このような場合の配信処理等では、コンテンツキー K_c や再生回路制限情報 $A_C 2$ が秘密復号鍵 K_{com} により暗号化されずに伝送され保持され、また、秘密復号鍵 K_{com} による暗号化処理および対応する復号処理が不要となる点を除いては、実施例 1～3 の動作と同様である。

10 このような構成とすることによって、秘密共通鍵 K_{com} に関する暗号化処理を行なわないような構成としても、実施例 1～3 に従うデータ配信システムと同様の効果を享受するデータ配信システムを構築することが可能である。

さらに、以上説明した実施例 1～3 において、以下のような変更を行うことも可能である。

15 まず、実施例 1～3においては、データ $\{K_c // A_C 2\} K_{com}$ (または、上述したように鍵 K_{com} を省略する構成では、データ $K_c // A_C 2$) を、公開暗号鍵 K_{Pm} (1) により再暗号化した上で、ライセンス情報保持部 1440 に記録する構成としていた。しかしながら、TRM 内に設けられるライセンス情報保持部 1440 に格納されるのであれば、必ずしも、公開暗号鍵 K_{Pm} (1) による再暗号化を行う必要はなく、再生情報の全てをライセンス情報保持部 1440 に記録するものとしても、実施例 1～3 と同様の効果が奏される。この場合、実施例 1 では、図 8 におけるステップ S148、図 12 におけるステップ S370 を、「トランザクション ID、コンテンツ ID、AC1、 $\{K_c // A_C 2\} K_{com}$ をライセンス情報保持部に記録する」と変更すればよい。また、実施例 2 では、図 17 におけるステップ S148、図 20 におけるステップ S370 を、実施例 3 では、図 24 におけるステップ S694 も、実施例 1 と同様に、「トランザクション ID、コンテンツ ID、AC1、 $\{K_c // A_C 2\} K_{com}$ をライセンス情報保持部に記録する」と変更すればよい。さらに、上記実施例 1～3 のいずれの変更に対しても、鍵 K_{com} を省略する構成とするのであれば、「トランザクション ID、コンテンツ ID、AC1、 $K_c // A_C 2$ をライセンス情報保持部に記録する」と

変更すればよい。

さらに、すべての実施例1～3のデータ配信システムでは配信サーバから再生情報の配信を受けるにあたって、メモリカードおよび携帯電話機（コンテンツ再生回路）の認証データ {K P m (1) } K P m a および {K P p (1) } K P m
5 a を、配信サーバに送信し（ステップS104）、配信サーバは受信（ステップS106）し、認証鍵K P m a にて復号（ステップS108）後、復号結果に従って、メモリカードと携帯電話機（コンテンツ再生回路）の双方に対する認証処理をするよう説明した。しかしながら、i) メモリカードは挿脱可能であることから、音楽を再生するのにコンテンツ再生回路が必ずしも配信を受けた携帯電話機である必然性がないこと、ii) 再生に際して、メモリカード内においても、再生情報の一部（ライセンスキーK c および再生回路制限情報A C 2）を出力するにあたって、出力先のコンテンツ再生回路の認証データ {K P m (1) } K P m a の認証処理を行っており、配信サーバにおけるコンテンツ再生回路の認証データ {K P m (1) } K P m a の認証処理を行わなくともセキュリティの低下につながらないことの2点から、配信サーバにおけるコンテンツ再生回路の認証データ {K P m (1) } K P m a の認証処理を行わない構成にしてもよい。
10
15

この場合、携帯電話機は、ステップS104にて、コンテンツIDとメモリカードの認証データ {K P m (1) } K P m a およびライセンス購入条件データA C を送信し、配信サーバは、ステップS106にて、コンテンツIDとメモリカードの認証データ {K P m (1) } K P m a およびライセンス購入条件データA C を送信し、ステップS108にて、認証データ {K P m (1) } K P m a を認証鍵K P m a にて復号して公開暗号鍵K P m (1) を受理する。続いて、ステップS110にて、復号結果に基づいて、あるいは認証サーバに問い合わせて、公開暗号鍵K P m (1) が正当な機器から出力されたものか否かを判断する認証処理を行い、メモリカードの認証データ {K P m (1) } K P m a の認証結果に従い、以降の処理を行うように変更するのみでよく、再生処理は何ら変更はない。
20
25

また、以上の説明では、配信された情報の格納は、メモリカードにより行われるものとしたが、本発明はこのような場合に限定されるものではない。すなわち、以上説明したようなメモリカードと同様の記録および暗号化などの機能を有する

のであれば、より一般的な記録装置にも適用可能である。このとき、記録装置は、携帯電話機のような通信装置にメモリカードのように着脱可能である構成にも必ずしも限定されず、通信装置に組み込まれる構成とすることも可能である。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定5となってはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

請求の範囲

1. 暗号化コンテンツデータの再生に関連し、前記暗号化コンテンツデータを復号して平文にするためのコンテンツキーを含む再生情報を、通信経路を介して受けて記録するためのメモリカード（110）であって、
 - 5 暗号化されて送られる前記再生情報の受信のために、前記再生情報の送信元との間での通信経路を確立するためのデータ通信部と、前記データ通信部から与えられる前記再生情報に関連するデータを保持するための第1の記憶部（1415, 1440）と、
 - 10 前記データ通信部からの前記再生情報に関連するデータを前記第1の記憶部へ格納する処理を行い、かつ前記第1の記憶部に格納されたデータに基づいて、前記再生情報を抽出するための情報抽出部と、前記再生情報の送信処理における処理状態を示す受信ログ情報を記録するための第2の記憶部（1460）と、
 - 15 前記メモリカードの動作を制御するための制御部（1420）とを備え、前記制御部は、要求に応じて前記受信ログ情報の前記送信元への送信を制御するメモリカード。
2. 前記データ通信部は、
 - 20 前記メモリカードに対応して予め定められた第1の公開暗号鍵によって暗号化されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部（1402）と、前記再生情報の通信ごとに更新されて送信され、前記第1の公開暗号鍵によって暗号化された第1の共通鍵を受けて、復号処理するための第1の復号処理部（1404）と、
 - 25 前記メモリカードごとに異なる第2の公開暗号鍵を保持するための第2の鍵保持部（1416）と、前記再生情報の通信ごとに更新して第2の共通鍵を生成する鍵生成部（1418）と、前記第2の公開暗号鍵および前記第2の共通鍵を、前記第1の共通鍵に基づい

て暗号化し、出力するための第1の暗号化処理部（1406）と、

前記第2の公開暗号鍵で暗号化され、さらに前記第2の共通鍵で暗号化された前記再生情報を受け、前記第2の共通鍵に基づいて復号するための第2の復号処理部（1412）とを含み、

5 前記第1の記憶部は、前記第2の復号処理部の出力に基づいたデータを保持し、前記情報抽出部は、

前記第2の公開暗号鍵によって暗号化されたデータを復号化するための第2の秘密復号鍵を保持する第3の鍵保持部（1421）と、

前記再生情報を関連するデータの前記第1の記憶部への格納処理から前記再生情報を抽出する処理までの過程において、前記第2の秘密復号鍵についての復号処理を行なう第3の復号処理部（1422）とを含む、請求項1記載のメモリカード。

3. 前記第1の記憶部は、

前記再生情報のうち前記コンテンツキーを含む一部である第1のデータを暗号化した状態で格納するための第3の記憶部（1415）と、

前記再生情報のうちの前記一部のデータを除く第2のデータを平文の状態で格納するための第4の記憶部（1440）とを含み、

前記情報抽出部は、前記第3の復号処理部が前記第2の復号処理部の出力に対して復号処理を行なった結果のうち、前記第2のデータを前記第4の記憶部に格納し、かつ

前記第3の復号処理部が前記第2の復号処理部の出力に対して復号処理を行なった結果のうちの一部を前記第2の公開暗号鍵で再び暗号化して、前記第3の記憶部に格納されるべき前記第1のデータを生成するための再暗号化処理部を含む、請求項2記載のメモリカード。

25 4. 前記第3の記憶部は、前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受けて格納する、請求項3記載のメモリカード。

5. 前記情報抽出部は、前記第3の復号処理部が前記第2の復号処理部の出力に対して復号処理を行なった結果を、平文の状態で前記第1の記憶部に格納する、請求項2記載のメモリカード。

6. 前記第1の記憶部は、

前記コンテンツキーに基づいて復号できる前記暗号化コンテンツデータを受け
て格納するための第3の記憶部(1415)と、

5 前記再生情報を平文の状態で格納するための第4の記憶部(1440)とを含
む、請求項5記載のメモリカード。

7. 前記メモリカードは、

前記再生情報の送信に先だって、前記再生情報の送信元にて認証処理を行なう
ための認証データを保持する第5の記憶部(1400)をさらに備え、

10 前記受信ログ情報は、前記認証処理において前記メモリカードが認証された場
合において、前記送信元から送信される前記再生情報の送信が行なわれるごとに
前記送信元で生成され、前記送信を特定するための通信特定情報と、前記第2の
共通鍵とを有する、請求項2記載のメモリカード。

8. 前記メモリカードは、

15 前記再生情報の送信に先だって、前記再生情報の送信元にて認証処理を行なう
ための認証データを保持する第5の記憶部(1400)をさらに備え、

前記受信ログ情報は、

前記認証処理において前記メモリカードが認証された場合において、前記送信
元から送信される前記再生情報の送信が行なわれるごとに前記送信元で生成され、
前記送信を特定するための通信特定情報と、

20 受信済みの前記再生情報の状態を示す状態情報と、

前記第2の共通鍵とを有し、

少なくとも前記状態情報と前記第2の共通鍵とに基づく署名情報を生成して出
力する手段をさらに備える、請求項2記載のメモリカード。

9. 前記第1の暗号化処理部は、前記受信ログ情報と前記署名情報をそれぞれ
25 前記第1の共通鍵に基づいて暗号化し、

前記メモリカードは、前記第1の暗号化処理部で個別に暗号化された前記受信
ログ情報と前記署名情報を前記送信元に返信する、請求項8記載のメモリカード。

10. 前記受信ログ情報は、前記コンテンツキーが前記第1の記憶部に格納され

るごとに、前記第2の記憶部から消去される、請求項1記載のメモリカード。

11. 前記受信ログ情報は、前記コンテンツキーの送信を前記送信元に対して要求するごとにオン状態とされ、前記コンテンツキーが前記第1の記憶部に格納されるごとに、オフ状態とされる受信状態フラグをさらに有する、請求項1記載のメモリカード。

12. データ配信システムであつて、

暗号化コンテンツデータと、暗号化コンテンツデータの再生に関連し、かつ前記暗号化コンテンツデータを復号して平文にするための復号鍵であるコンテンツキーを含む再生情報とを供給するためのコンテンツデータ供給装置を備え、

10 前記コンテンツデータ供給装置(10)は、

前記コンテンツデータおよび前記再生情報を保持するための配信情報保持部(304)と、

外部との間でデータを授受するための第1のインターフェース部(350)と前記端末に対する前記再生情報の配信ごとに更新される第1の共通鍵を生成する第1のセッションキー発生部(316)と、

前記ユーザの端末に対応して予め定められた第1の公開暗号鍵により前記第1の共通鍵を暗号化して前記第1のインターフェース部に与えるためのセッションキー暗号化部(318)と、

前記第1の共通鍵により暗号化されて返信される第2の公開暗号鍵と第2の共通鍵とを復号するためのセッションキー復号部(320)と、

前記暗号化コンテンツデータを再生するための再生情報を、前記セッションキー復号部により復号された前記第2の公開暗号鍵によって暗号化するための第1のライセンスデータ暗号処理部(326)と、

前記第1のライセンスデータ暗号処理部の出力を前記第2の共通鍵でさらに暗号化して前記第1のインターフェース部に与え配信するための第2のライセンスデータ暗号処理部(328)と、

前記配信処理中の処理状態を示す配信ログ情報を記録するための配信ログ情報保持部(306)とを含み、

前記コンテンツデータ供給装置から、通信経路を介して配信を受けるために複

数のユーザにそれぞれ対応する複数の端末（100）をさらに備え、

各前記端末は、

外部との間でデータ授受をするための第2のインターフェース部（1104）と、

前記暗号化コンテンツデータと前記再生情報とを受けて格納するデータ格納部

（110）とを含み、

前記データ格納部は、

前記データ格納部に対応して予め定められた第1の公開暗号鍵によって暗号化

されたデータを復号化するための第1の秘密復号鍵を保持する第1の鍵保持部

（1402）と、

前記再生情報の通信ごとに更新されて配信され、前記第1の公開暗号鍵によつ

て暗号化された第1の共通鍵を受けて、復号処理するための第1の復号処理部

（1404）と、

前記データ格納部ごとに異なる第2の公開暗号鍵を保持するための第2の鍵保

持部（1416）と、

前記再生情報の通信ごとに更新して第2の共通鍵を生成する鍵生成部（141

8）と、

前記第2の公開暗号鍵および前記第2の共通鍵を、前記第1の共通鍵に基づい
て暗号化し、出力するための第1の暗号化処理部（1406）と、

前記第2の公開暗号鍵で暗号化され、さらに第2の共通鍵で暗号化された再生

20 情報を受け、前記第2の共通鍵に基づいて復号するための第2の復号処理部（1
412）と、

前記第2の復号処理部の出力に基づいたデータを保持する第1の記憶部（14
15, 1440）と、

前記第2の公開暗号鍵によって暗号化されたデータを復号化するための第2の

25 秘密復号鍵を保持する第3の鍵保持部（1421）と、

前記再生情報に関連するデータの前記第1の記憶部への格納処理から前記再生
情報抽出する処理までの過程において、前記第2の秘密復号鍵についての復号
処理を行なう第3の復号処理部（1422）と、

前記暗号化コンテンツデータおよび前記再生情報の配信処理における処理状態

を示す受信ログ情報を記録するための第2の記憶部(1460)と、

外部との間のデータ授受を制御する受信制御部(1420)とを有し、

前記受信制御部は、前記配信処理中に前記通信経路が切断された場合に、前記受信ログ情報に基づいて再配信処理を制御する、データ配信システム。

5 13. 前記データ格納部は、前記端末に着脱可能なメモリカードである、請求項12記載のデータ配信システム。

14. 前記コンテンツデータ供給装置は、

前記再生情報の配信に先だって、前記メモリカードから送信される認証データにより前記メモリカードを認証する手段(312)と、

10 前記再生情報の配信処理を行なうごとに、前記配信処理を特定するための配信特定情報を生成する手段(315)とをさらに備え

前記メモリカードは、

前記認証データを保持する第3の記憶部(1460)をさらに備え、

15 前記受信ログ情報は、前記認証処理において前記メモリカードが認証された場合において、送信元から送信される、前記再生情報の送信が行なわれるごとに前記送信元で生成され、前記送信を特定するための通信特定情報と前記第2の共通鍵とを有する、請求項13記載のデータ配信システム。

16. 前記受信ログ情報は、前記再生情報が前記第1の記憶部に格納されるごとに、前記第2の記憶部から消去される、請求項12記載のデータ配信システム。

20 16. 前記受信ログ情報は、前記再生情報の配信を前記送信元に対して要求するごとにオン状態とされ、前記再生情報が前記第1の記憶部に格納されるごとに、オフ状態とされる受信状態フラグを含む、請求項12記載のデータ配信システム。

17. 前記受信ログ情報は、少なくとも前記通信特定情報と前記第2の共通鍵を有する、請求項12記載のデータ配信システム。

FIG. 1

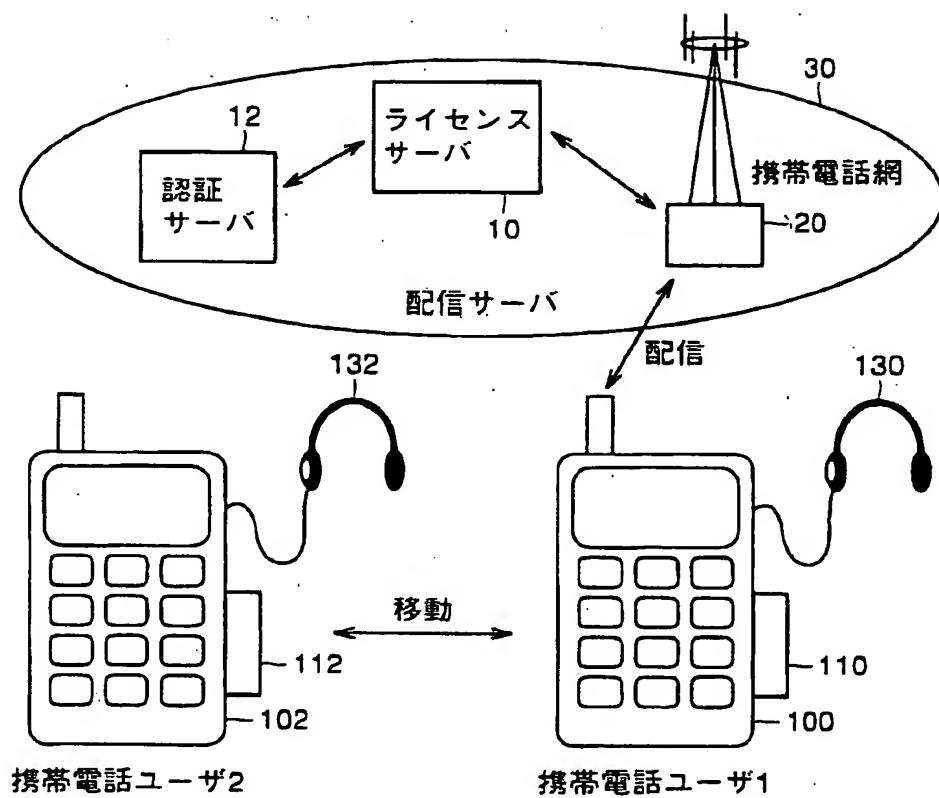


FIG.2

名称	機能・特徴	保持・ 発生箇所
Data	コンテンツデータ、Kcにて復号可能な暗号化を施した暗号化コンテンツデータとして{Data}Kcの形式にて配布	配信サーバ
Data-inf	付加情報、コンテンツデータに関する著作権連あるいはサーバアクセス連等の平文情報	配信サーバ
Kc	コンテンツ復号キー	配信サーバ
Kp(n)/Kmc(n)	コンテンツ再生／メディアのクラス(種類等)に依存する復号鍵	携帯電話機 メモリカード
KPp(n)/KPmc(n)	Kp/Kmcにて復号可能な非対称暗号化鍵、認証機能を有する。 (KPp)KPma/(KPp)KPmaの形式で出荷時に記録	携帯電話機 メモリカード
Kcom	再生回路共通の秘密復号鍵、暗号化されたKc,AC2の復号に利用 (非対称 配信サーバKPcom／再生回路Kcom も良い)	配信サーバ 携帯電話機
KPma	システム共通の認証鍵(公開)	配信サーバ
AC	利用者側からのライセンスに対する購入条件(機能限定、ライセンス数 etc)	携帯電話機
AC1	メモリのアクセスに対する制限情報	配信サーバ
AC2	再生回路における制御情報	配信サーバ
Km(i)	メモリカード毎に固有の復号鍵(iはカードを識別する識別子)	メモリカード
KPm(i)	Km(i)にて復号可能な非対称な公開暗号鍵	メモリカード
Ks1	配信セッション毎に発生するセッション固有の共通鍵	配信サーバ
Ks2	配信／移動(受)セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks3	再生セッション毎に発生するセッション固有の共通鍵	メモリカード
Ks4	再生セッション毎に発生するセッション固有の共通鍵	携帯電話機
コンテンツID	コンテンツデータDataを識別するコード	配信サーバ
トランザクションID	ライセンスの発行を特定できる管理コード(コンテンツIDをも含めて識別することも考えられる)	配信サーバ

30

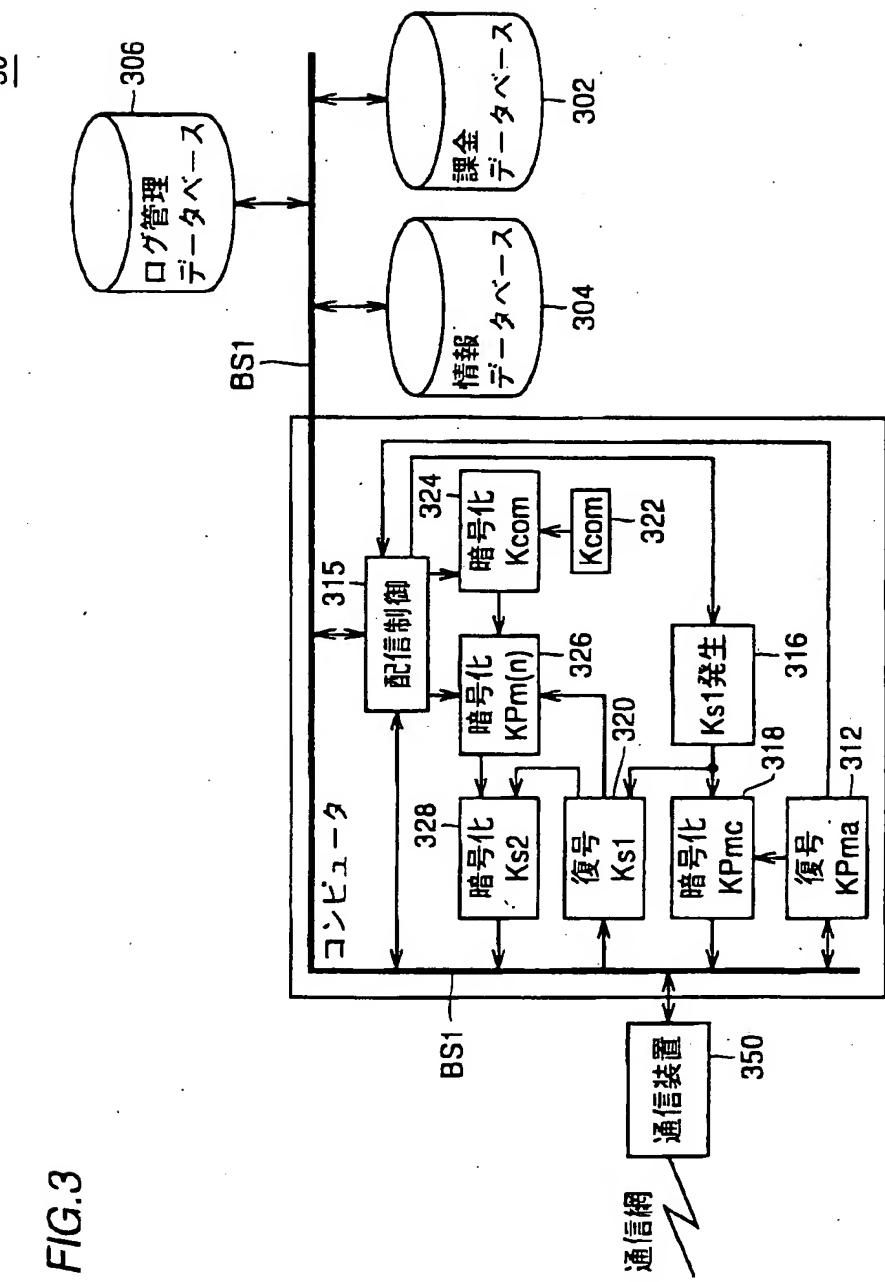


FIG.3

100
 FIG.4

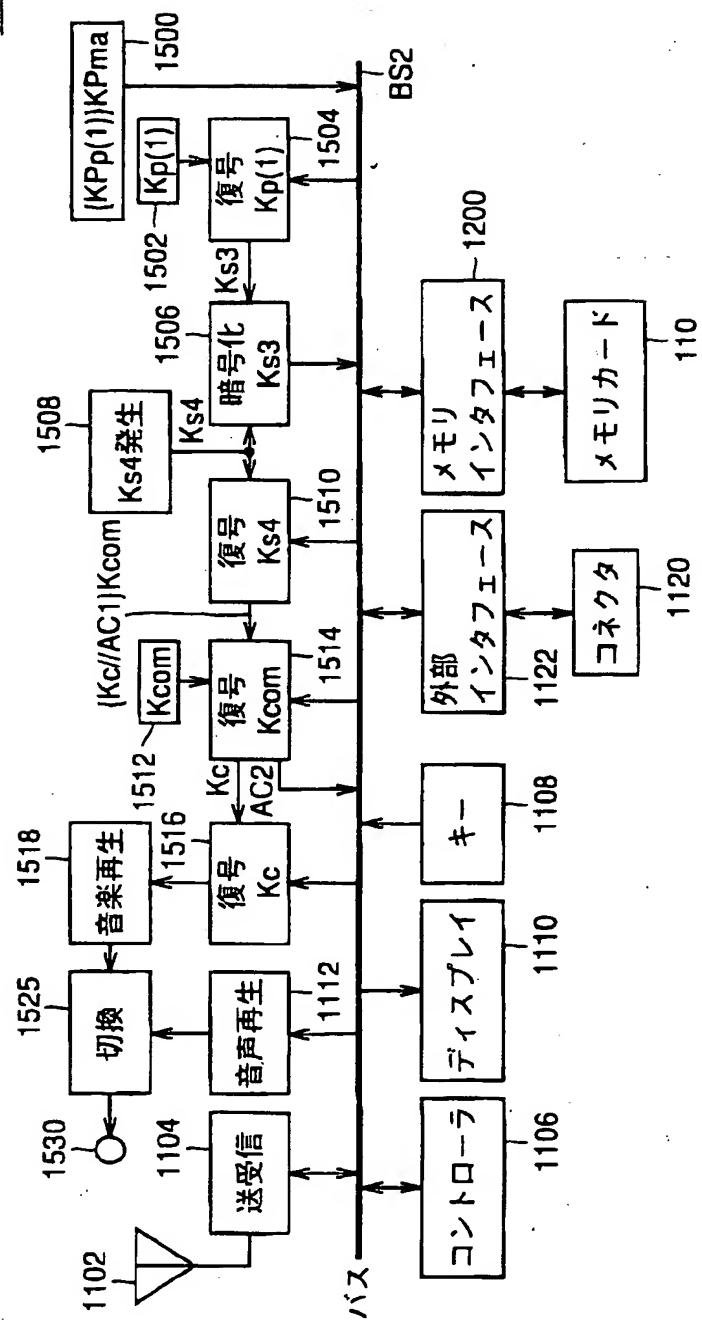


FIG. 5

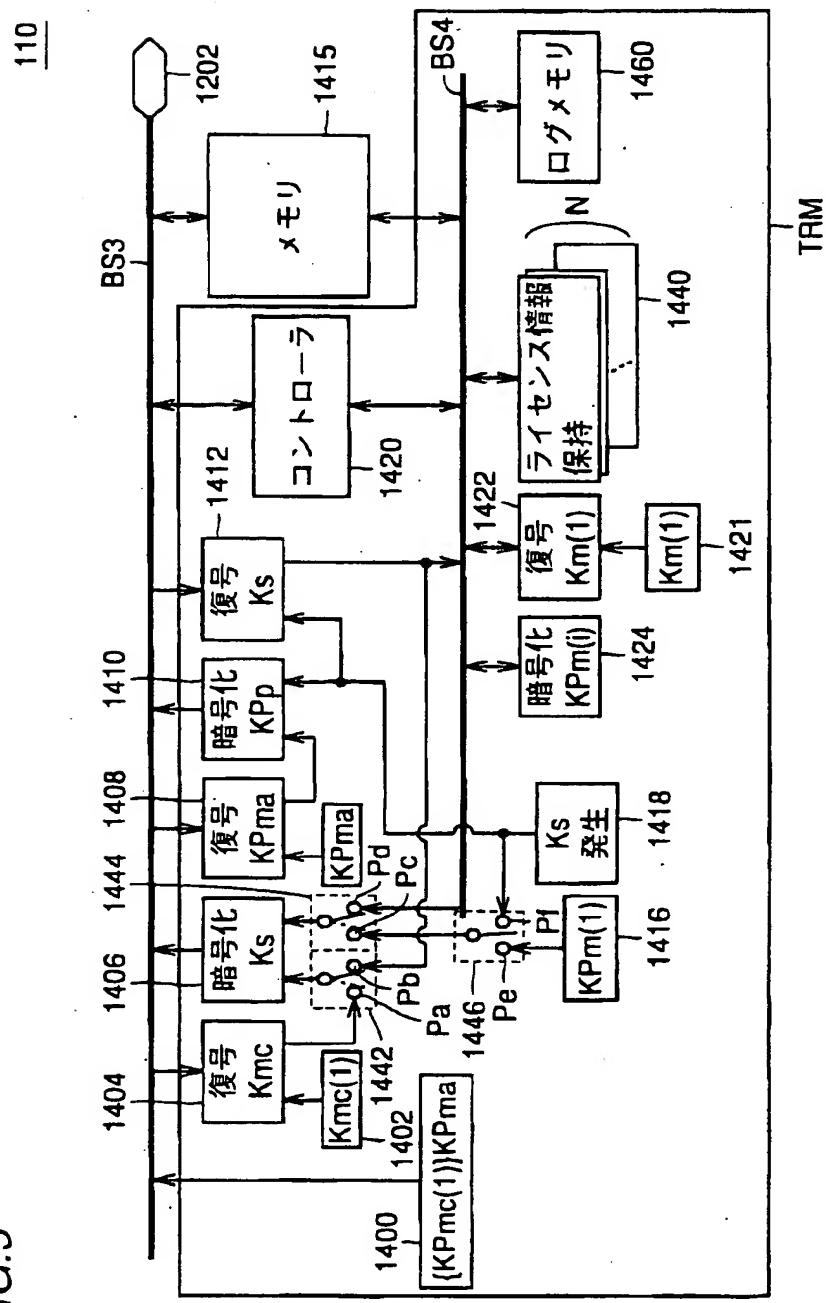


FIG. 6

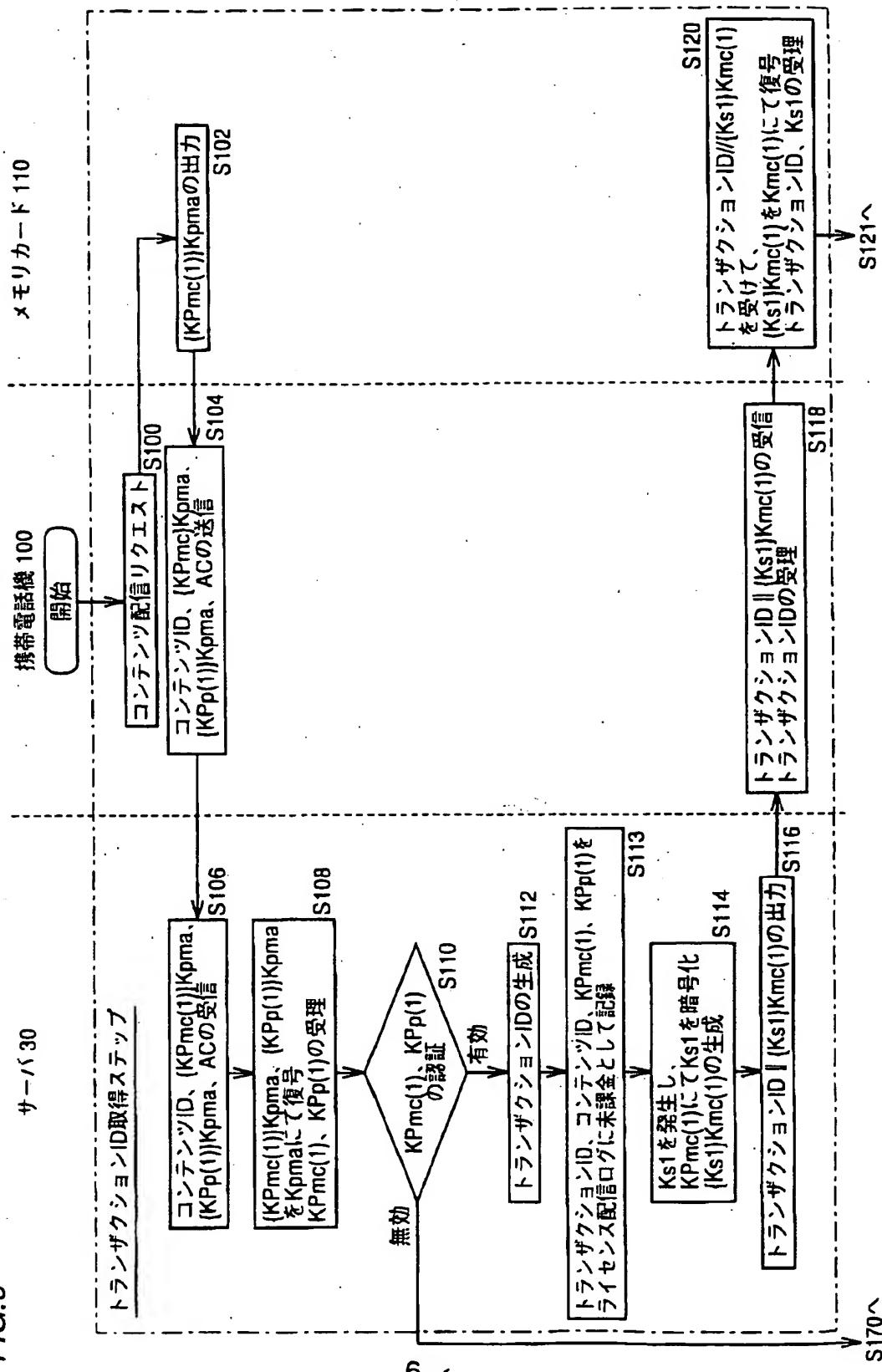


FIG.7 サーバ30
S110から 携帯電話機 100
メモリカード 110
S120から

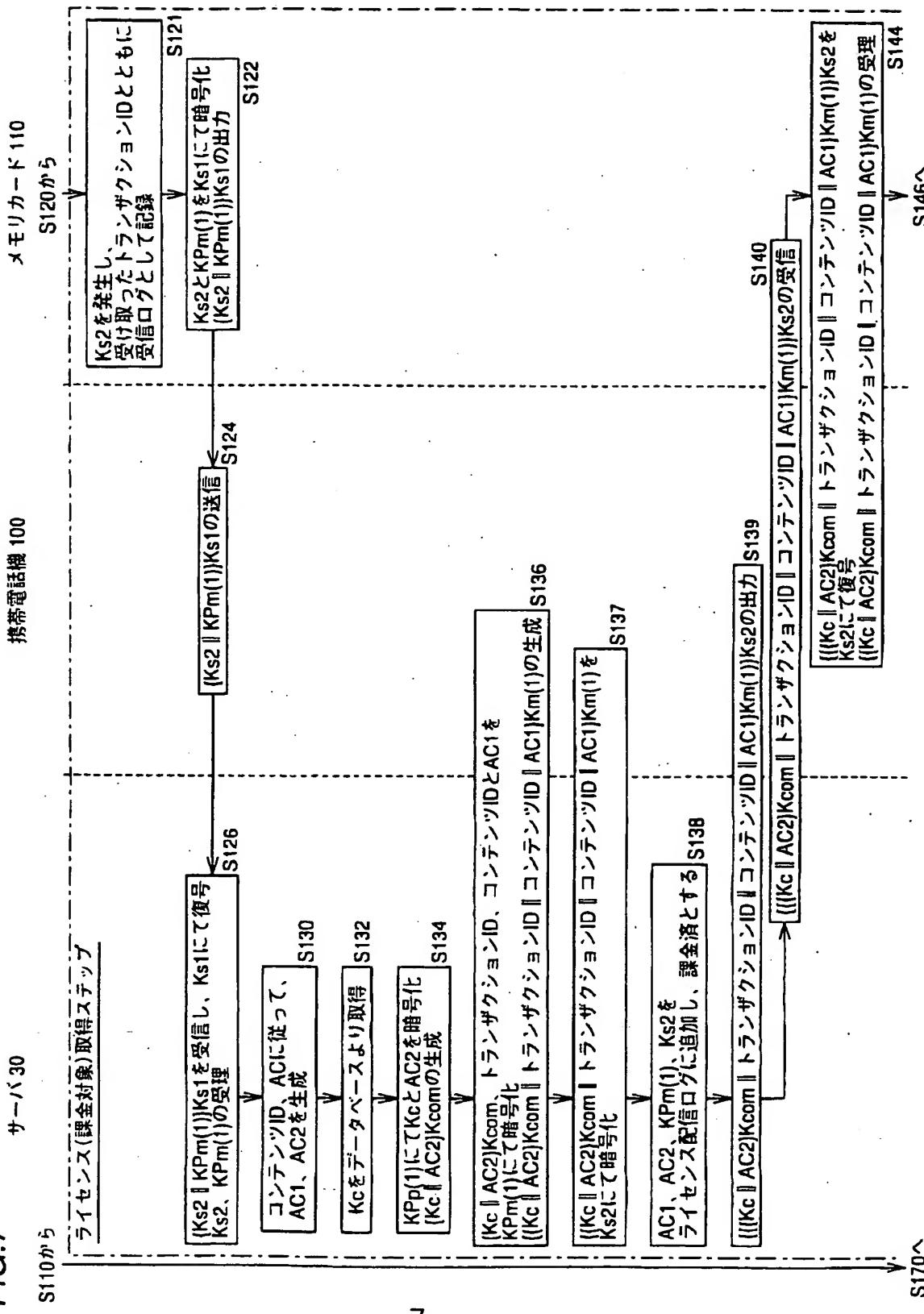
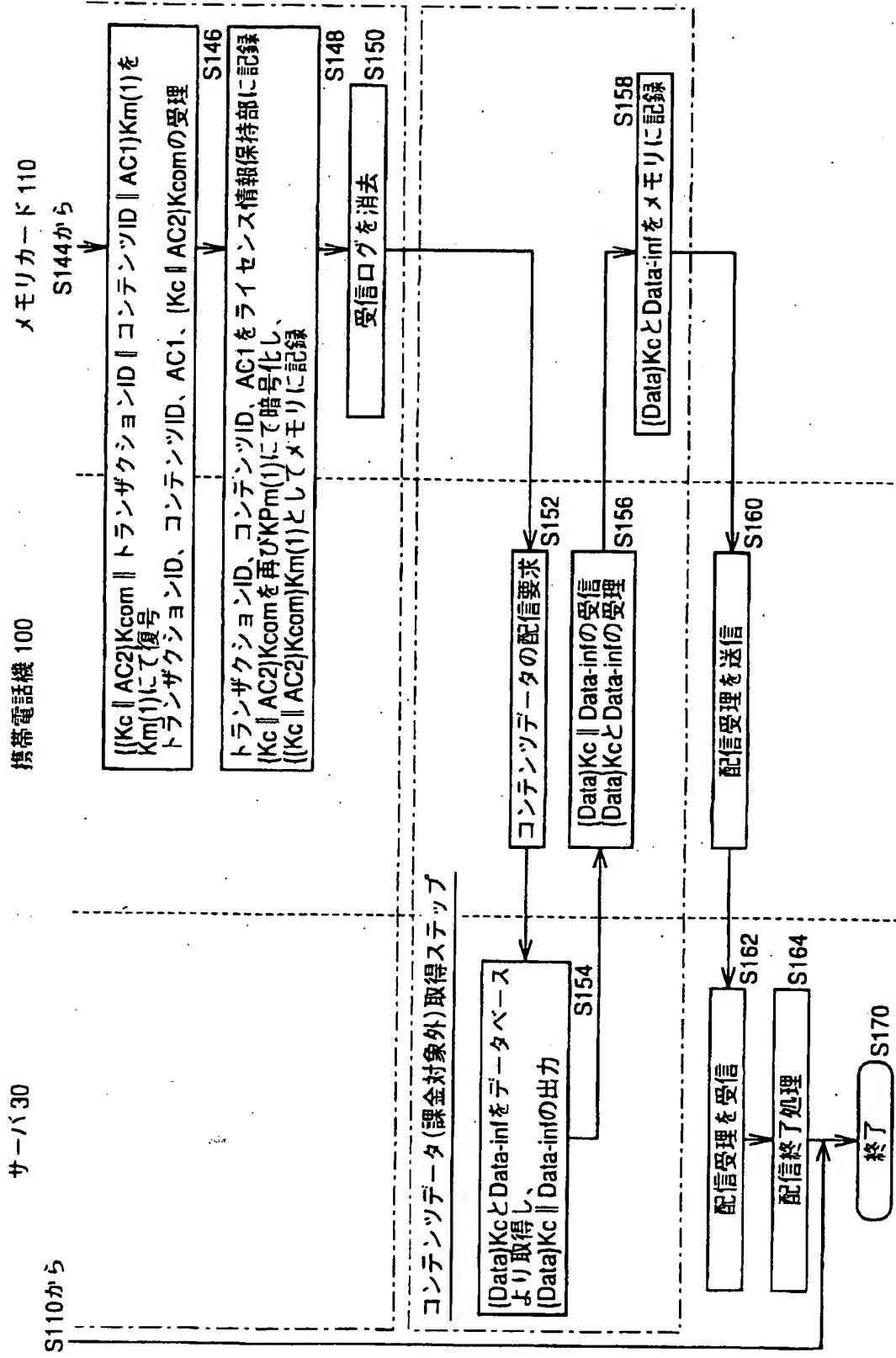


FIG.8



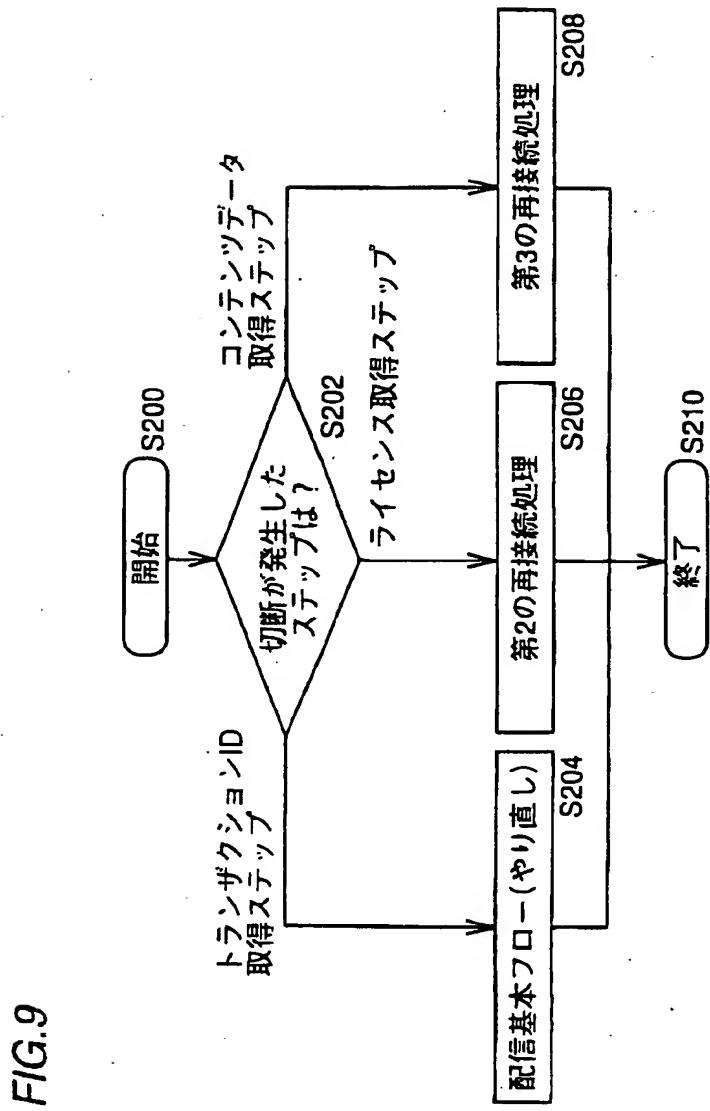


FIG.9

FIG.10 サーバ30

携帯電話機 100 メモリカード 110

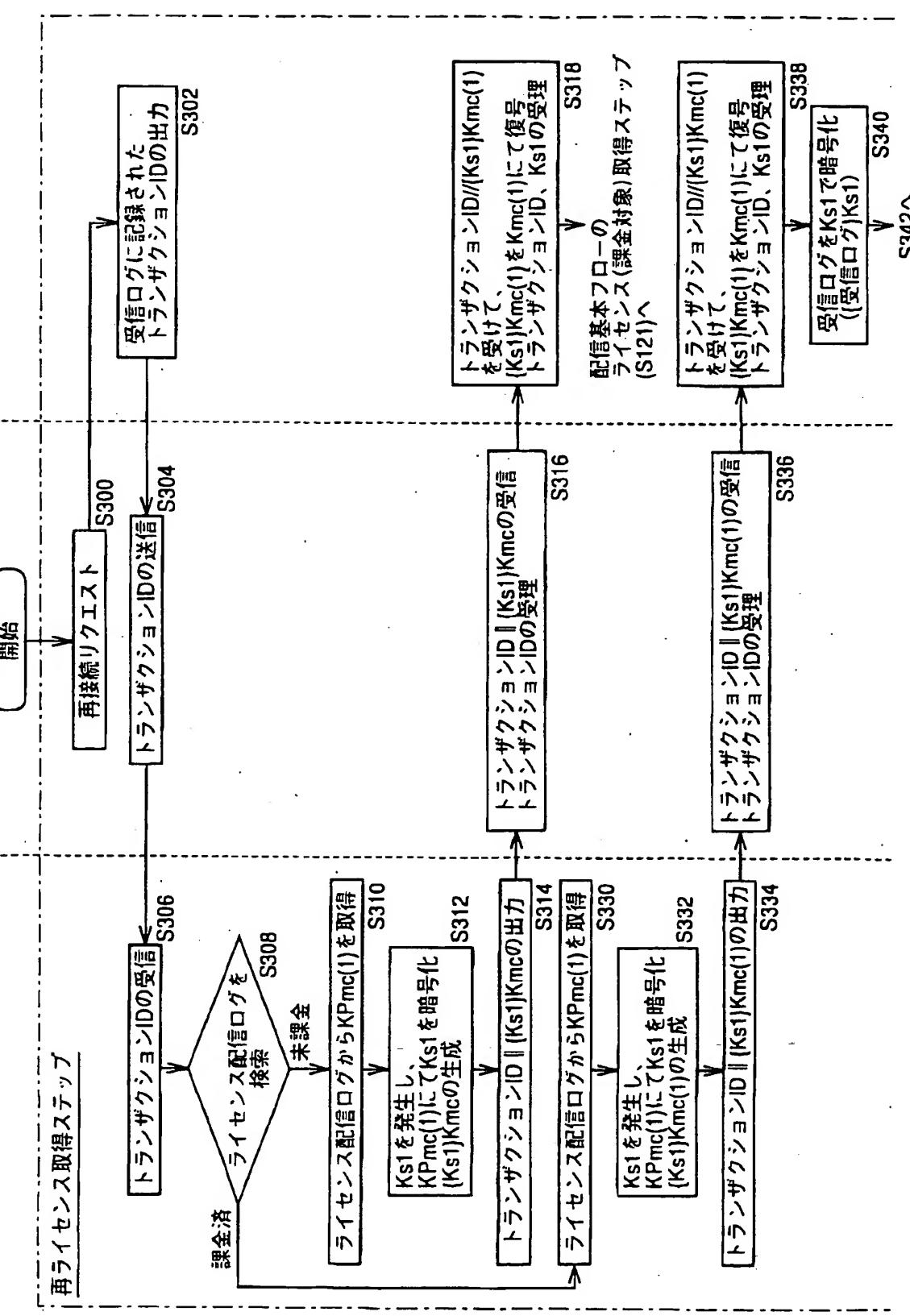


FIG.11

サーバ30

携帯電話機100

メモリカード110

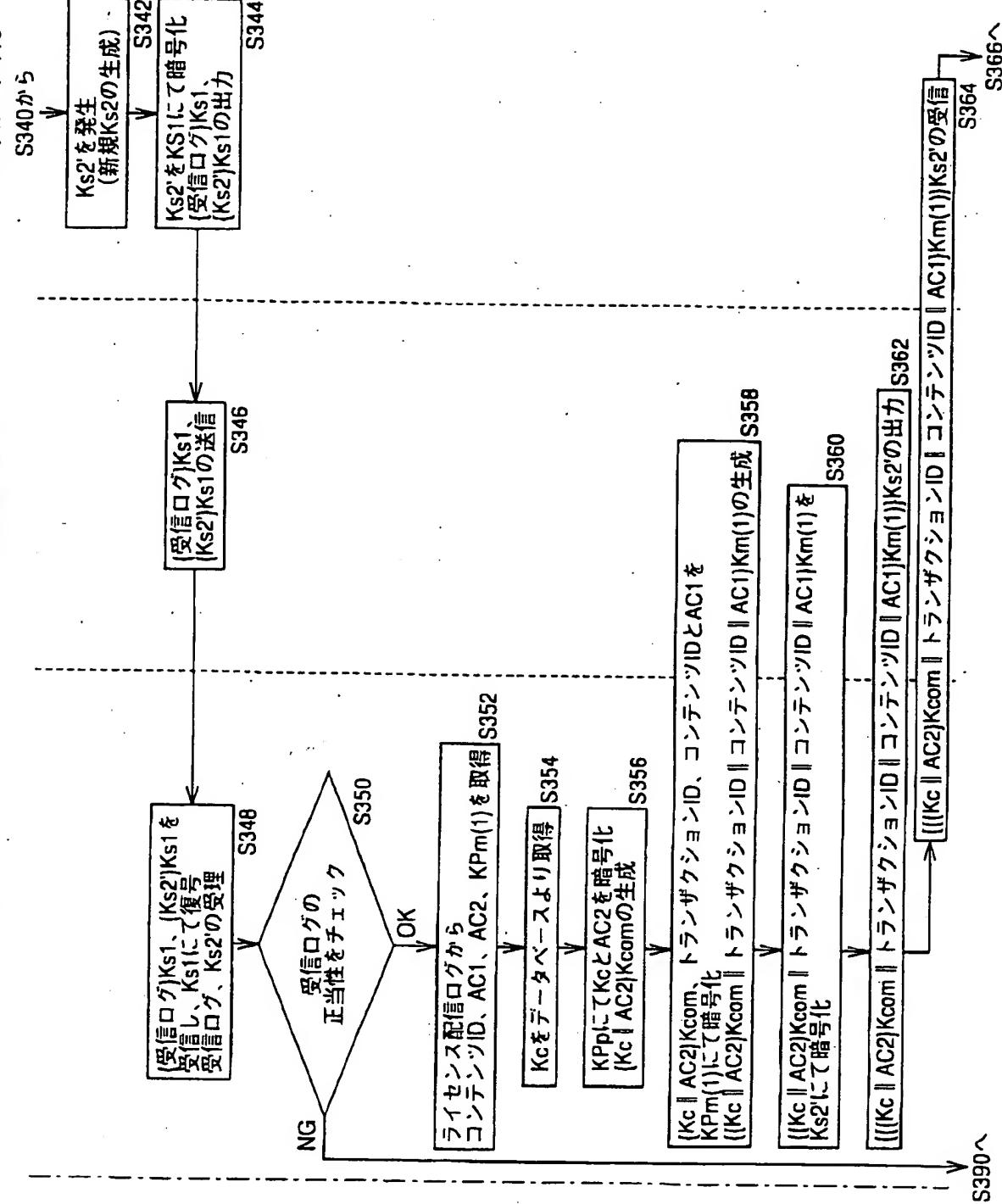


FIG. 12

携帯電話機 100 サーバ 30

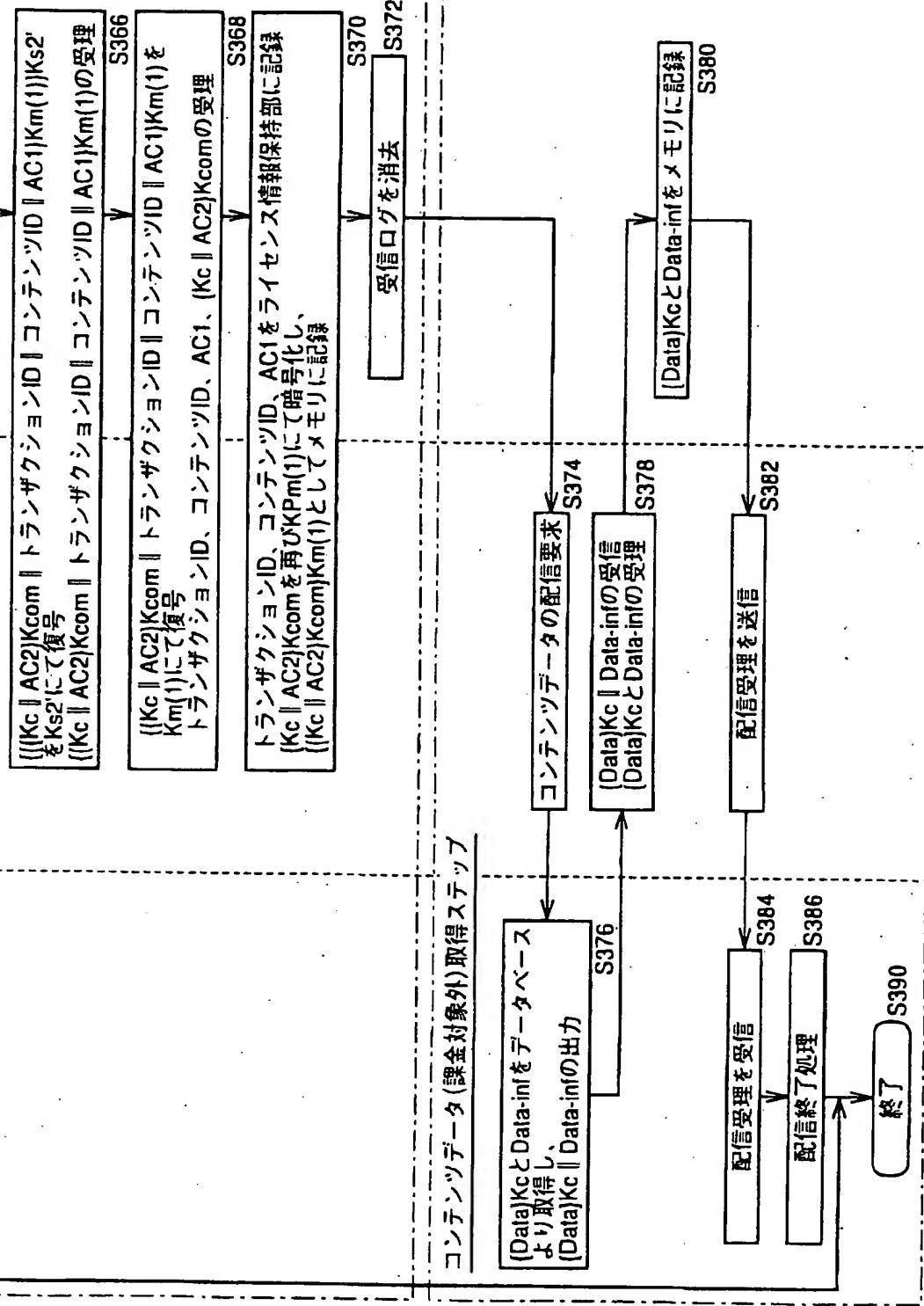
メモリカード 110
S350 から
↓
S364 から

FIG.13

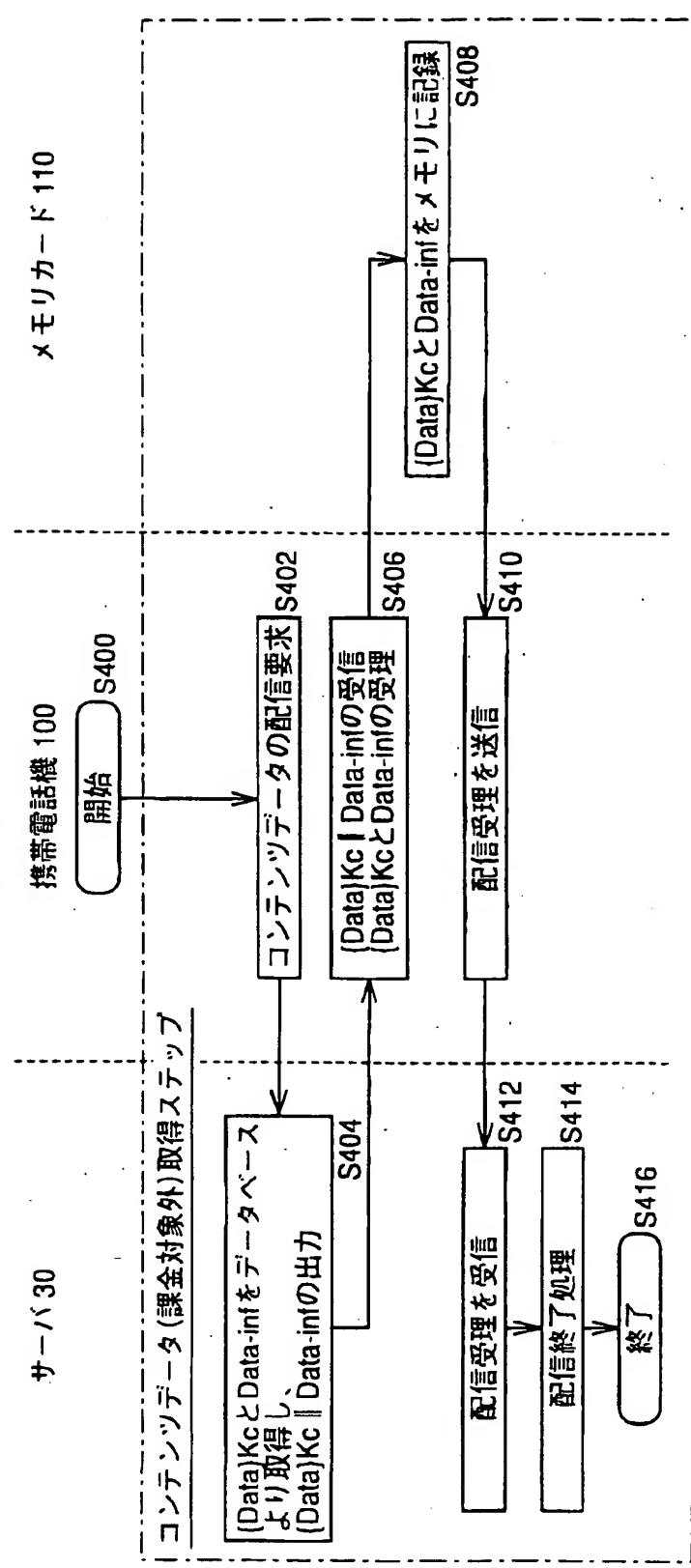


FIG. 14

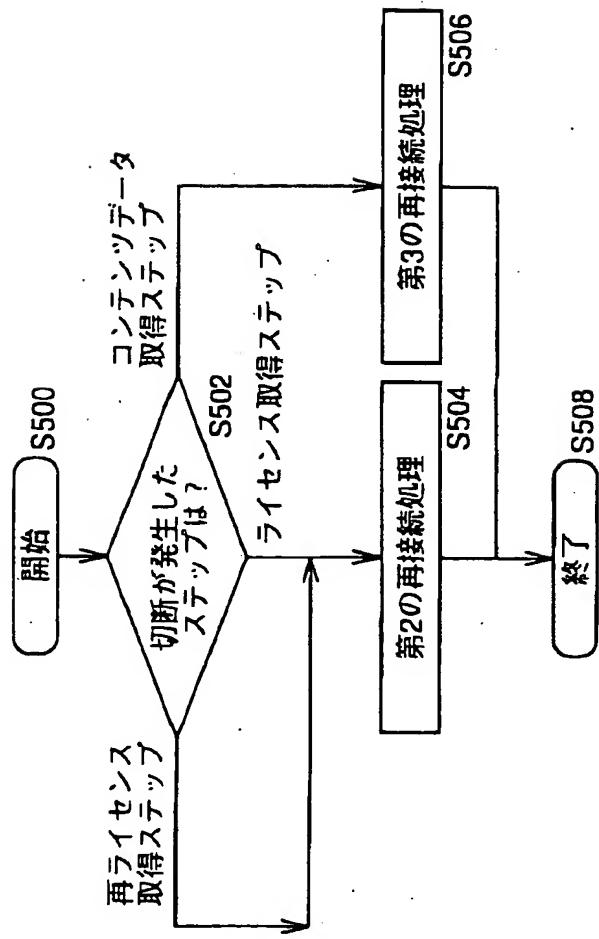


FIG. 15

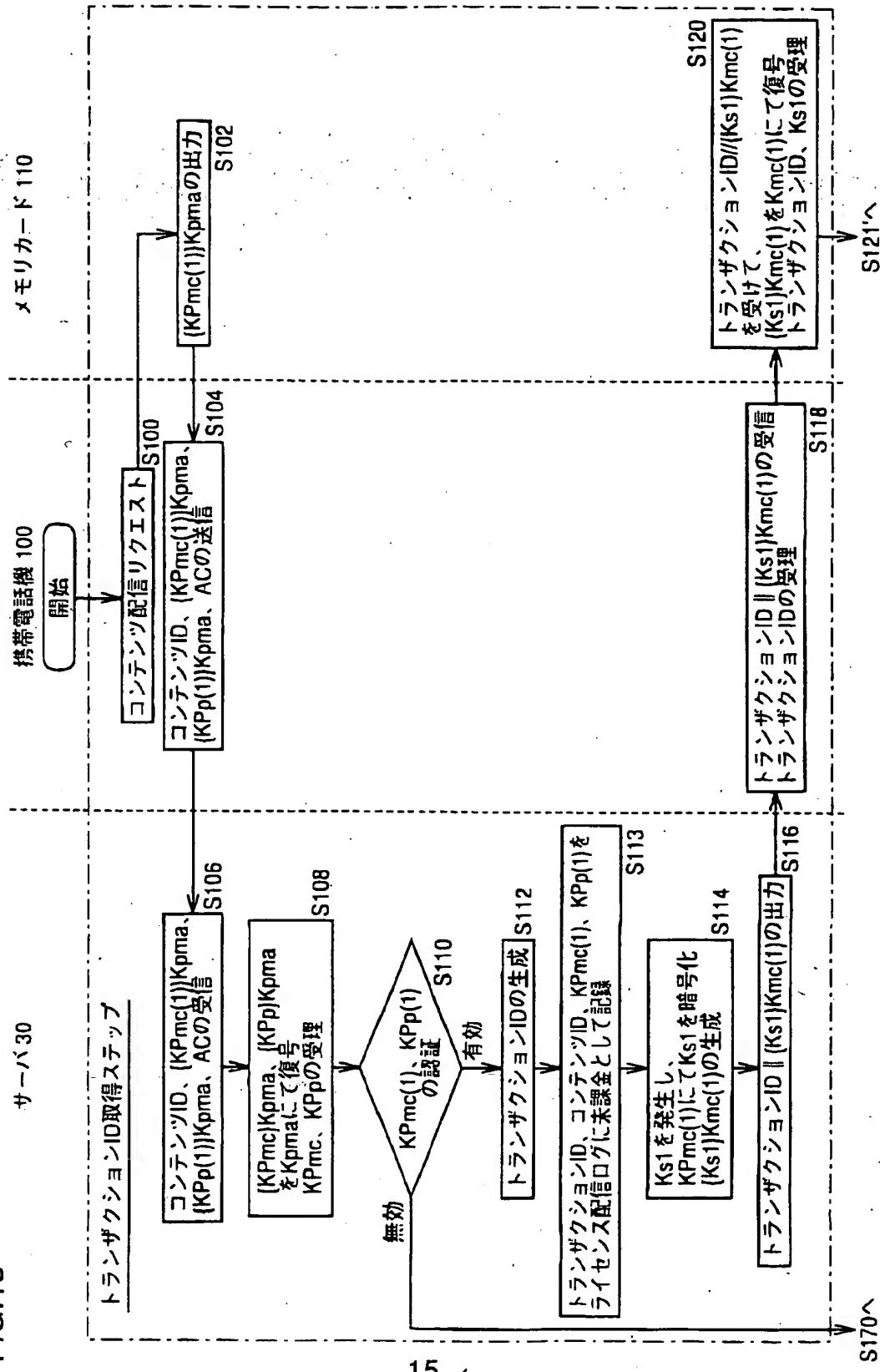


FIG. 16

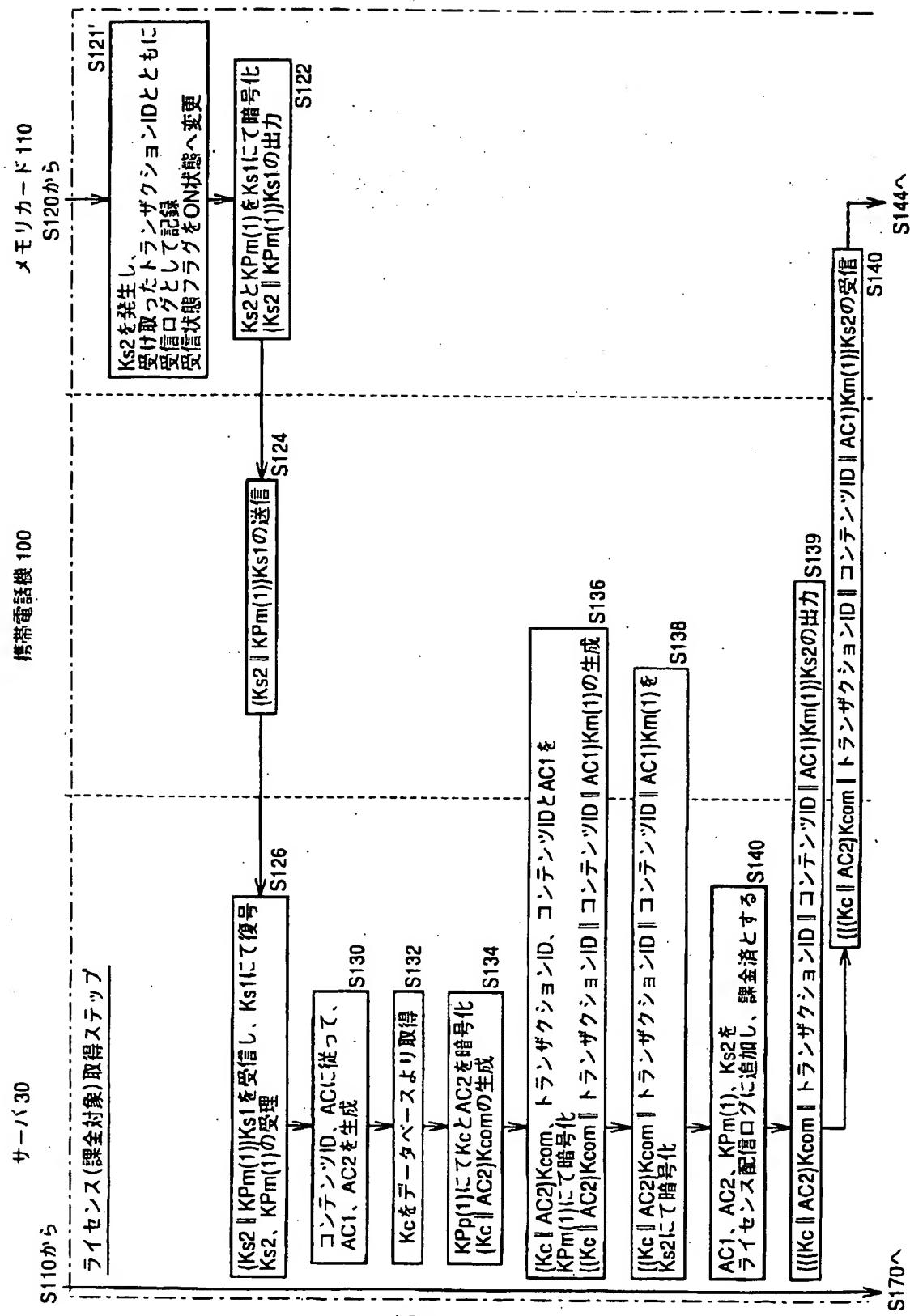


FIG. 17

サーバ30
S110から

携帯電話機100

メモリカード110

S140から

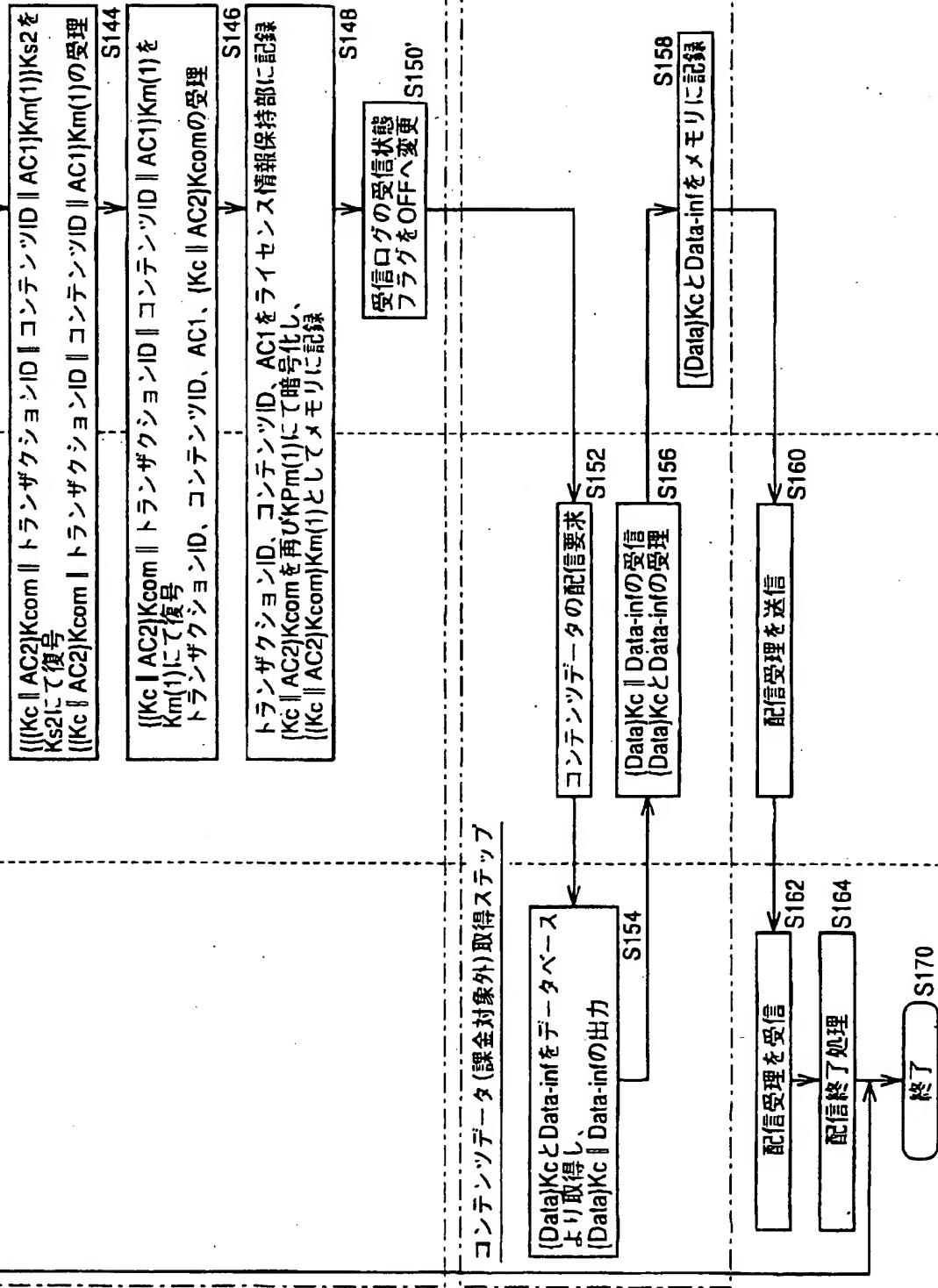


FIG.18

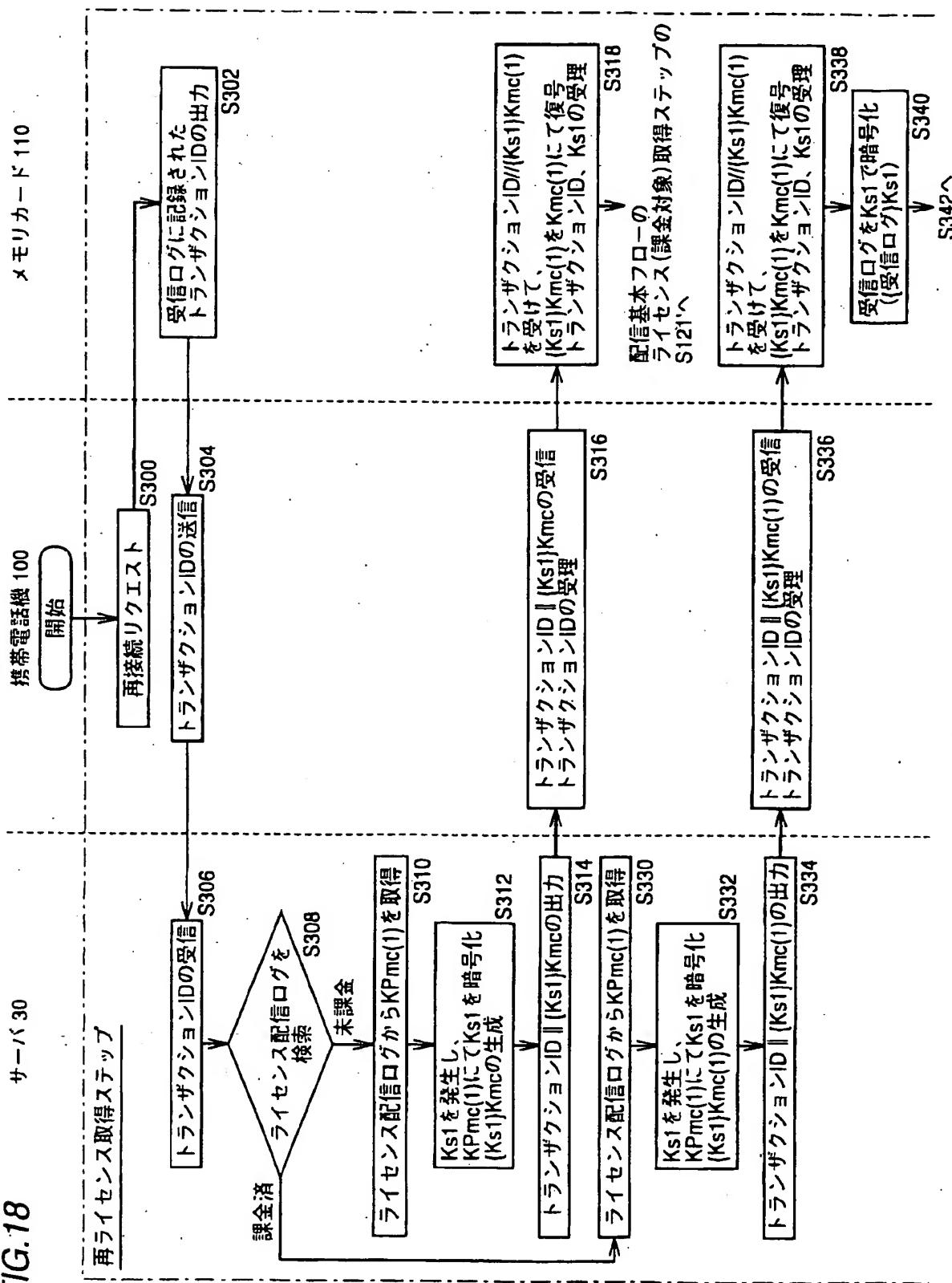
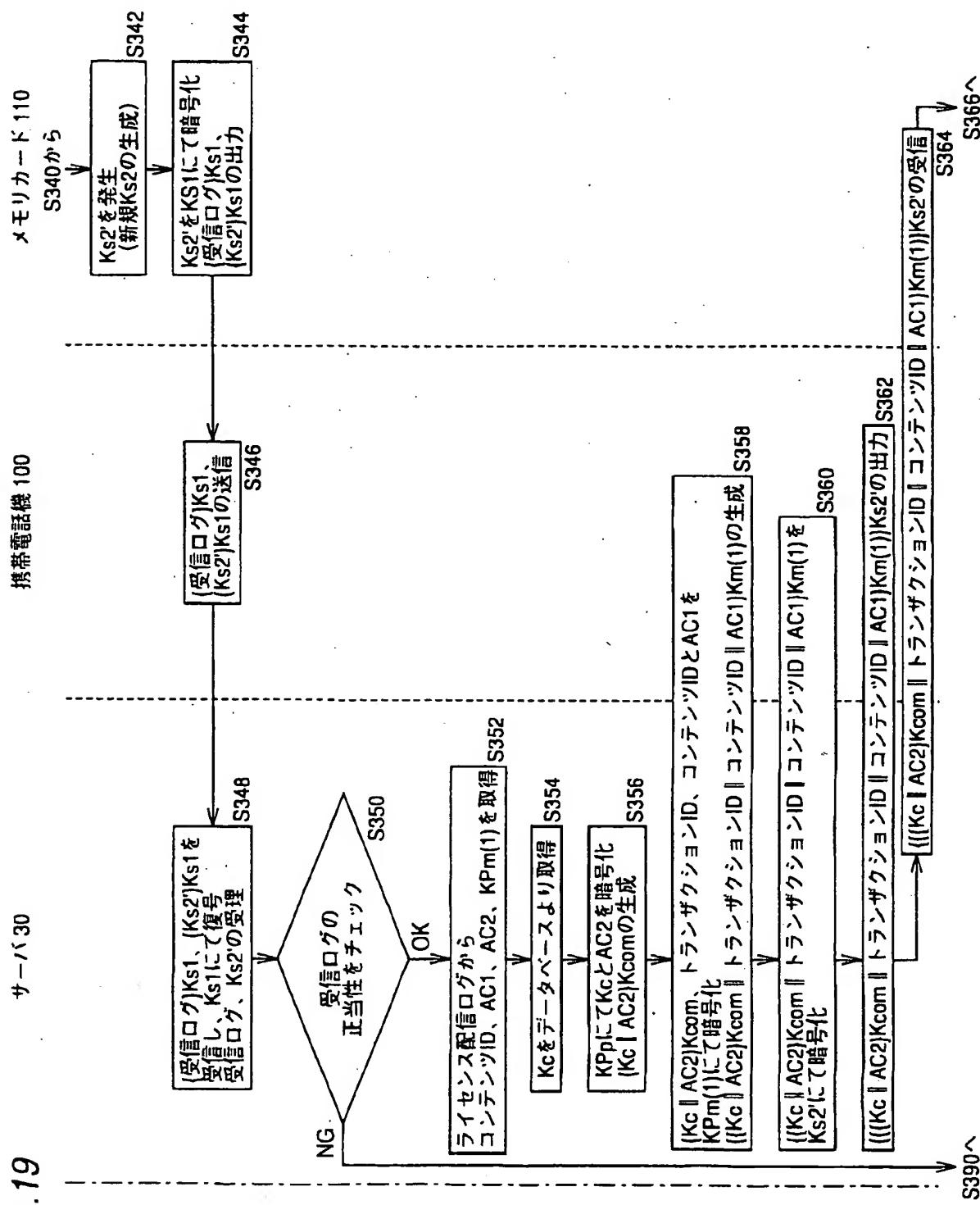


FIG.19

サーバ30 携帯電話機 100



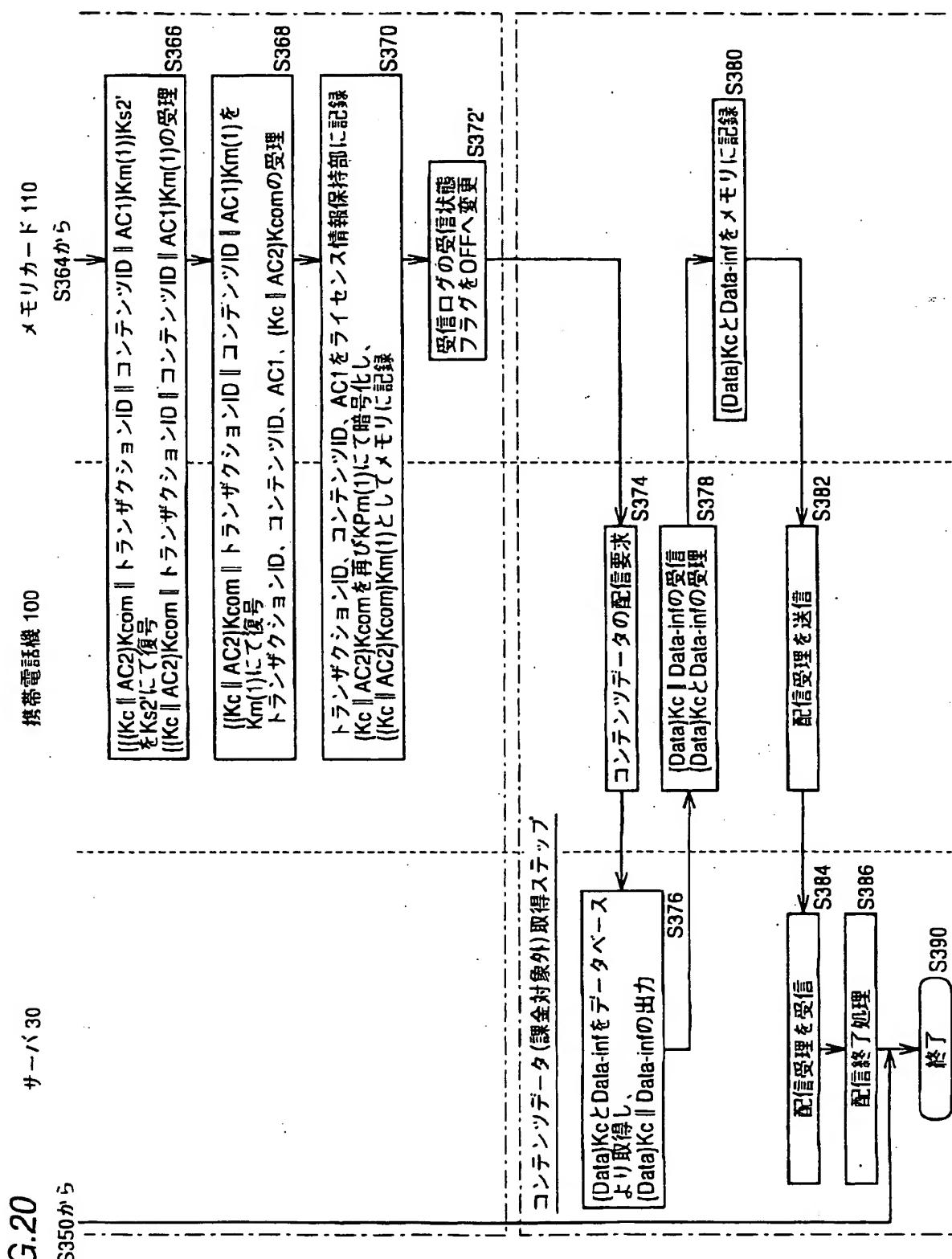
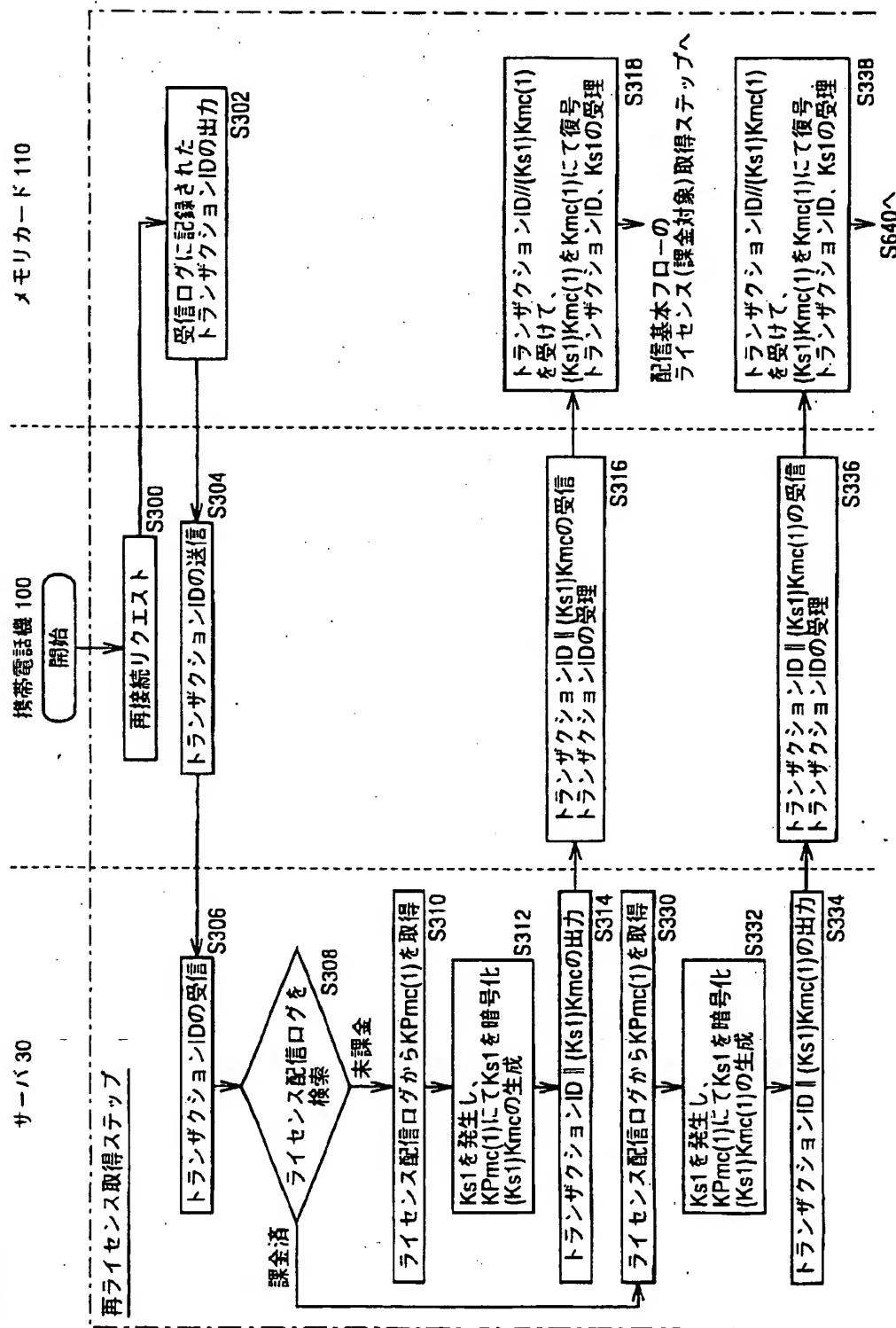


FIG. 21



サーバ30 携帯電話機100

FIG.22

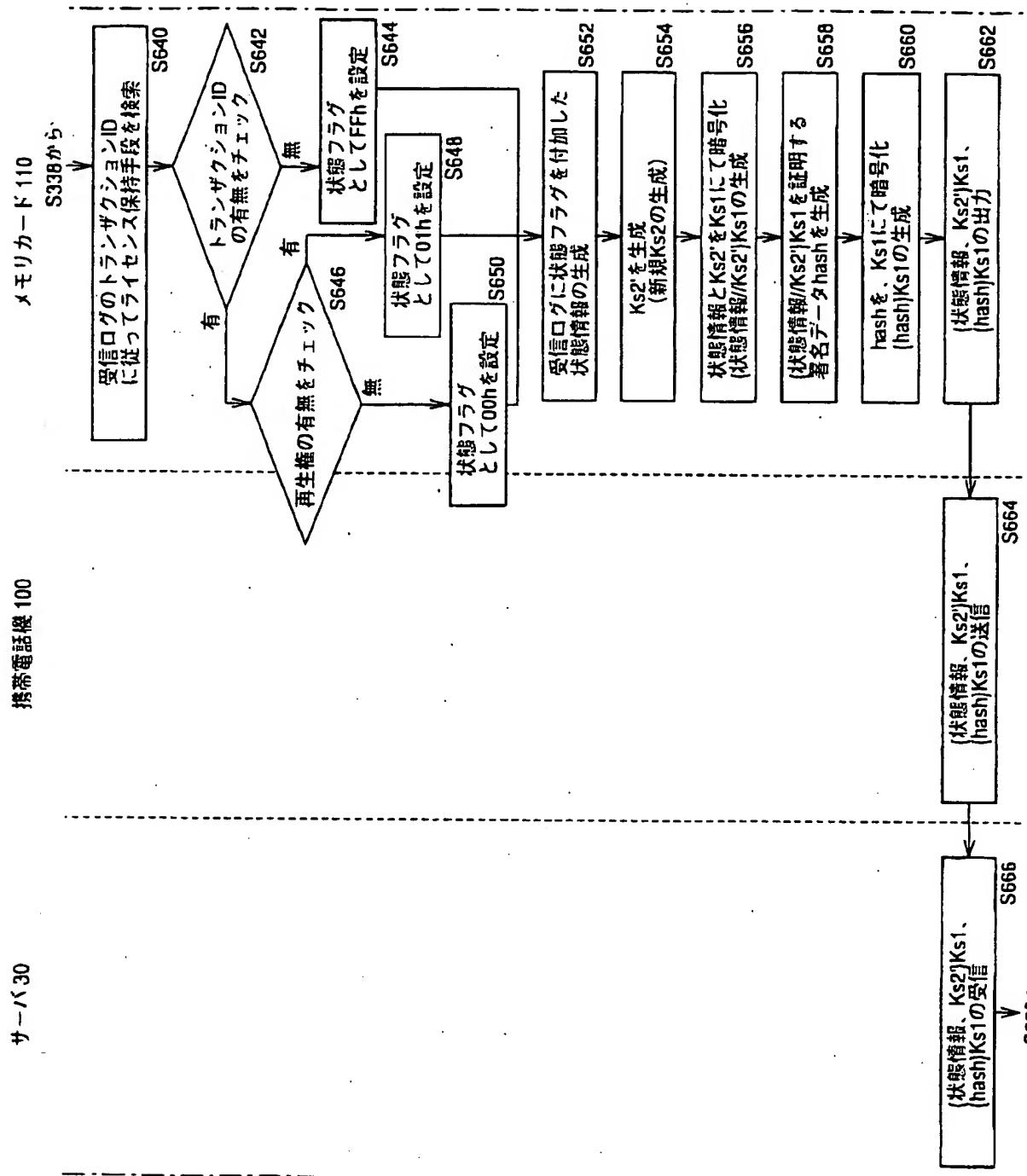


FIG.23

携帯電話機 100

メモリカード 110

サーバ 30
S666から△ (hash)Ks1をKs1にて
復号して、状態情報の正当性
をチェック

OK

[状態情報 // (Ks2)Ks1をKs1にて復号
状態情報、Ks2の受理]

S668

△ 再送信の
正当性をチェック

OK

ライセンス配信ログから
コンテンツID、AC1、AC2、KPm(1)を取得

S670

△ Kcをデータベースより取得
KPpにてKcとAC2を暗号化
[Kc || AC2]Kcomの生成

S674

[Kc || AC2]Kcom、トランザクションID、コンテンツIDとAC1を
[Kp || AC2]Kcomにて暗号化
[Kc || AC2]Kcom || トランザクションID || コンテンツID || AC1]Km(1)の生成

S680

[Kc || AC2]Kcom || トランザクションID || コンテンツID || AC1]Km(1)を
[Ks2]にて暗号化

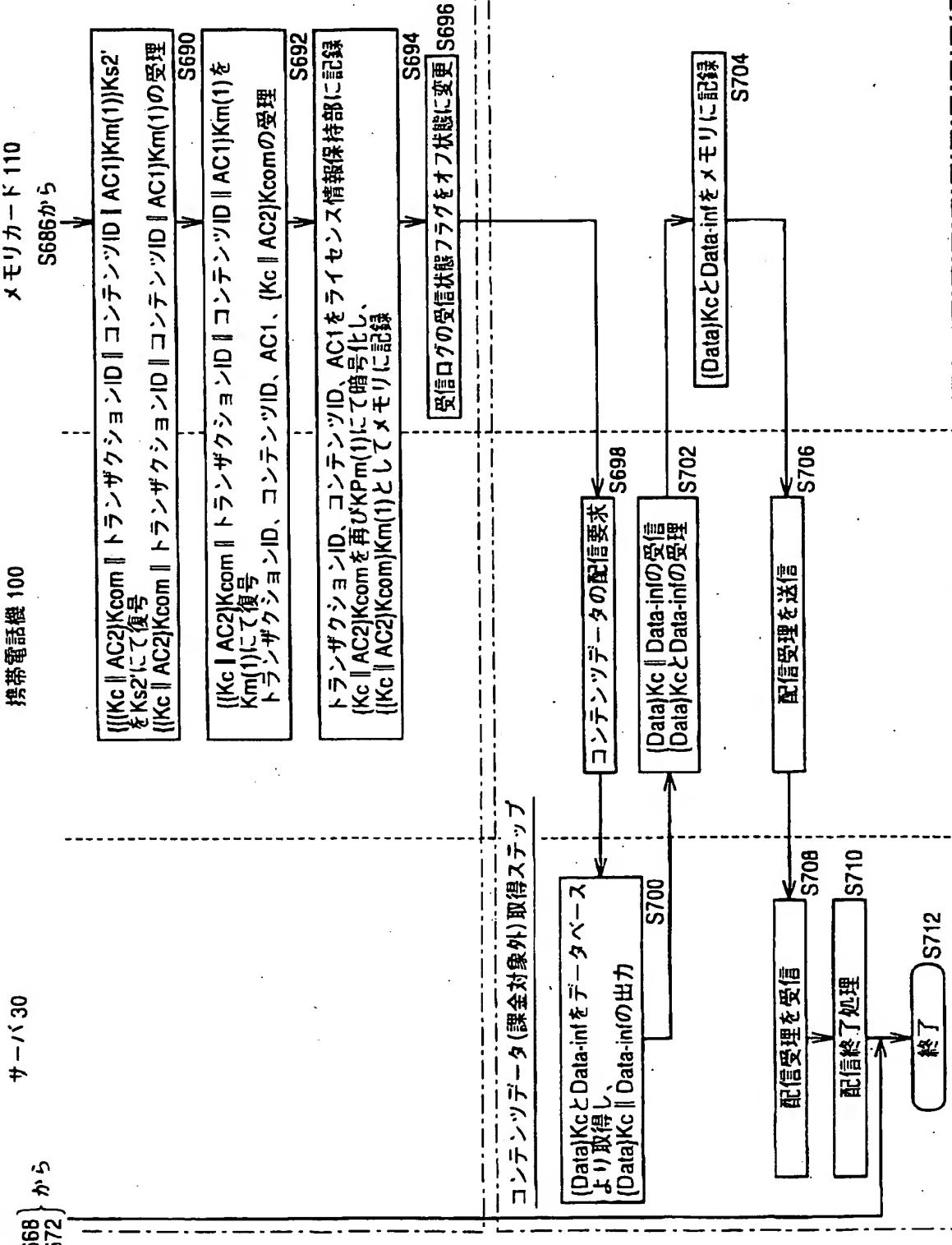
S682

[[[Kc || AC2]Kcom || トランザクションID || コンテンツID || AC1]Km(1) || Ks2]の出力

S684

S686
S688へ

FIG.24



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/08544

A. CLASSIFICATION OF SUBJECT MATTER
 Int.Cl⁷ H04L 9/10 G06F 12/14, G10K 15/02 G06F 13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
 G06F 12/00-13/00 G10K 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
 Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
 JICST FILE (JOIS)
 WPI (DIALOG)
 INSPEC (DIALOG)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 11-224288, A (Hitachi, Ltd.), 17 August, 1999 (17.08.99) & EP, 935209, A2 & SG, 75914, A1 & CA, 2260536, A1	1-17
EA	JP, 2000-253453, A (Sony Corporation), 14 September, 2000 (14.09.00) & EP, 1033894, A2 & CN, 1266326, A	1-17
EA	JP, 2000-268096, A (Dainippon Printing Co., Ltd.), 29 September, 2000 (29.09.00) (Family: none)	1-17

Further documents are listed in the continuation of Box C. See patent family annex.

"A"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E"	earlier document but published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means	"&"	document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
 08 March, 2001 (08.03.01)

Date of mailing of the international search report
 21 March, 2001 (21.03.01)

Name and mailing address of the ISA/
 Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

国際調査報告

国際出願番号 PCT/JPOO/08544

A. 発明の属する分野の分類(国際特許分類(IPC))

Int. C17
H04L 9/10 G06F 12/14, G10K 15/02 G06F 13/00

B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. C17
H04L 9/00 H04K 1/00-3/00 G09C 1/00-5/00
G06F 12/00-13/00 G10K 15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
日本国公開実用新案公報 1971-2001年
日本国登録実用新案公報 1994-2001年
日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)
WPI (DIALOG)
INSPEC (DIALOG)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 11-224288, A (株式会社日立製作所) 17. 8月. 1999 (17. 08. 99) & EP, 935209, A2 & SG, 75914, A1 & CA, 2260536, A1	1-17
EA	JP, 2000-253453, A (ソニー株式会社) 14. 9月. 2000 (14. 09. 00) & EP, 1033894, A2 & CN, 1266326, A	1-17

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとつて自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 08. 03. 01	国際調査報告の発送日 21.03.01
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官(権限のある職員) 丸山 高政 印 電話番号 03-3581-1101 内線 3574

C (続き) 関連すると認められる文献		関連する 請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
EA	JP, 2000-268096, A (大日本印刷株式会社) 29. 9月. 2000 (29. 09. 00), (ファミリーなし)	1-17